

03-06-00

A



Attorney's Docket No.: U 012638-5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application  
Assistant Commissioner for Patents  
Washington, D.C. 20231

PATENT



NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of Inventors:

1. YOUNGDONG WU
2. HUIJIE ROBERT DENG
3. FENG BAO

**WARNING:** The Declaration must name all of the actual inventor(s).

For (title):

REMOTE AUTHENTICATION BASED ON EXCHANGING SIGNALS REPRESENTING BIOMETRICS INFORMATION

1. Type of Application

This new application is for a(n) (check one applicable item below):

- ☒ Original (nonprovisional)
- ☐ Design
- ☐ Plant

**WARNING:** Do not use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. 371(c)(4) unless the International Application is being filed as a divisional, continuation or continuation-in-part application.

CERTIFICATION UNDER 37 CFR 1.10

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service on this date **MARCH 3, 2000** in an envelope as "Express Mail Post Office to Addressee" Mailing Label Number **EL386267783US** addressed to the: Assistant Commissioner of Patents, Washington, D.C. 20231

IBIS CARRILLO

(type or print name of person mailing paper)

(Signature of person mailing paper)

**NOTE:** Each paper or fee referred to as enclosed herein has the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 CFR 1.10(b).

**WARNING:** Certificate of mailing (first class) or facsimile transmission procedures of 37 CFR 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

**WARNING:** Do not use this transmittal for the filing of a provisional application.

## 2. Benefit of Prior U.S. Application(s) (35 U.S.C. 119(e), 120, or 121)

**NOTE:** If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

**WARNING:** If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. 120, 121 or 365(c). (35 U.S.C. 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. 119, 365(a) or 365(b).) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.

**WARNING:** When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional **must** be filed prior to the Saturday, Sunday or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).

- ☐ The new application being transmitted claims the benefit of prior U.S. application(s) and enclosed are **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

**NOTE:** If one of the following 3 items apply, then complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED** and a **NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION**.

- ☐ Divisional.  
☐ Continuation.  
☐ Continuation-in-Part (C-I-P).

## 3. Papers Enclosed That Are Required For Filing Date Under 37 CFR 1.53 (Regular) or 37 CFR 1.153 (Design) Application

27 Pages of specification

20 Pages of claims

1 Pages of Abstract

7 Sheets of drawing

- ☒ formal  
☐ informal

**WARNING:** **DO NOT** submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. Comments on proposed new 37 CFR 1.84. Notice of March 9, 1988 (1990 O.G. 57-62).

**NOTE:** "Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm. (5/8 inch) down from the top of the page." 37 C.F.R. 1.84(c).

(complete the following, if applicable)

- ☐ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)". 37 C.F.R. 1.84(b).

**4. Additional papers enclosed**

- ☒ Preliminary Amendment
- ☐ Information Disclosure Statement (37 CFR 1.98)
- ☐ Form PTO-1449
- ☐ Citations
- ☐ Declaration of Biological Deposit
- ☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.
- ☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative
- ☐ Special Comments
- ☐ Other

**5. Declaration or oath**

- ☒ Enclosed
- executed by *(check all applicable boxes)*
- ☒ inventors.
- ☐ legal representative of inventors. 37 CFR 1.42 or 1.43
- ☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.
- ☐ This is the petition required by 37 CFR 1.47 and the statement required by 37 CFR 1.47 is also attached. *See item 13 below for fee.*
- ☐ Not Enclosed.

**WARNING:** Where the filing is a completion in the U.S. of an International Application but where a declaration is not available or where the completion of the U.S. application contains subject matter in addition to the International Application the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.

- ☐ Application is made by a person authorized under 37 CFR 1.41(c) on behalf of *all the above named inventors*. (The declaration or oath, along with the surcharge required by 37 CFR 1.16(e) can be filed subsequently).

**NOTE:** It is important that all the correct inventor(s) are named for filing under 37 CFR 1.41(c) and 1.53(b).

- ☐ Showing that the filing is authorized. *(Not required unless called into question. 37 CFR 1.41(d).)*

**6. Inventorship Statement**

**WARNING:** If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.

The inventorship for all the claims in this application are:

- ☐ The same
- ☐ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

7. **Language**

*NOTE: An application including a signed oath or declaration may be filed in a language other than English. A verified English translation of the non-English language application and the processing fee of \$130.00 required by 37 CFR 1.17(k) is required to be filed with the application or within such time as may be set by the Office. 37 CFR 1.52(d).*

*NOTE: A non-English oath or declaration in the form provided or approved by the PTO need not be translated. 37 CFR 1.69(b).*

- ☒ English  
☐ non-English  
☐ the attached translation is a verified translation. 37 CFR 1.52(d).

8. **Assignment**

- ☒ An assignment of the invention to KENT RIDGE DIGITAL LABS.  
☒ is attached. A separate ☒ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.  
☐ will follow.

*NOTE: "If an assignment is submitted with a new application, send two separate letters—one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).*

*WARNING: A newly executed "CERTIFICATE UNDER 37 CFR 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993. 1150 O.G. 62-64.*

9. **Certified Copy**

Certified copy of application

Country	Appln. No.	Filed
Singapore	9906598-9	December 24, 1999

from which priority is claimed

- ☐ is attached.  
☒ will follow.

*NOTE: The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 CFR 1.55(a) and 1.63.*

*NOTE: This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. 120 is itself entitled to priority from a prior foreign application then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.*

10. **Fee Calculation (37 CFR 1.16)**

- A. ☒ Regular Application

---

Claims as Filed

---

Number Filed	Number Extra			Rate	Basic Fee 37 CFR 1.16(a) \$690.00
Total Claims (37 CFR 1.16(c))	74	- 20	= 54	x \$ 18.00	972.00
Independent Claims (37 CFR 1.16(b))	12	- 3	= 9	x \$ 78.00	702.00
Multiple dependent claim(s), if any (37 CFR 1.16(d))				+ \$ 260.00	

- ☐ Amendment cancelling extra claims enclosed.
- ☒ Amendment deleting multiple-dependencies enclosed.
- ☒ Fee for extra claims is not being paid at this time.

**NOTE:** *If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 CFR 1.16(d).*

Filing Fee Calculation \$ 690.00

- B. ☐ Design application  
(\$310.00 — 37 CFR 1.16(f))

Filing Fee Calculation \$

- C. ☐ Plant application  
(\$480.00 — 37 CFR 1.16(g))

Filing Fee Calculation \$

**11. Small Entity Statement(s)**

- ☐ Verified Statement(s) that this is a filing by a small entity under 37 CFR 1.9 and 1.27 is(are) attached or has been filed.

Filing Fee Calculation (50% of **A**, **B** or **C** above) \$

**NOTE:** *Any excess of the full fee paid will be refunded if a verified statement and a refund request are filed within 2 months of the date of timely payment of a full fee. 37 CFR 1.28(a).*

**12. Request for International-Type Search (37 CFR 1.104(d)) (Complete, if applicable)**

- ☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

**13. Fee Payment Being Made At This Time**

- ☐ Not Enclosed
- ☐ No filing fee is to be paid at this time. *(This and the surcharge required by 37 CFR 1.16(e) can be paid subsequently.)*

- ☒ Enclosed

☒ basic filing fee \$ 690.00

- ☒ Recording assignment  
(\$40.00; 37 CFR 1.21(h)) (See attached "COVER SHEET FOR ASSIGNMENT ACCOMPANYING NEW APPLICATION.")
- ☐ Petition fee for filing by other than all the inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached.  
(\$130.00; 37 CFR 1.47 and 1.17(h)) \$
- ☐ For processing an application with a specification in a non-English language.  
(\$130.00; 37 CFR 1.52(d) and 1.17(k)) \$
- ☐ Processing and retention fee  
(\$130.00; 37 CFR 1.53(d) and 1.21(l))
- ☐ Fee for international-type search report  
(\$40.00; 37 CFR 1.21(e)). \$

*NOTE: 37 CFR 1.21(l) establishes a fee for processing and retaining any application which is abandoned for failing to complete the application pursuant to 37 CFR 1.53(d) and this, as well as the changes to 37 CFR 1.53 and 1.78, indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid or the processing and retention fee of §1.21(l) must be paid within 1 year from notification under §53(d).*

Total fees enclosed \$ 690.00

#### 14. Method of Payment of Fees

- ☒ Check in the amount of \$ 690.00
  - ☐ Charge Account No. 12-0425 in the amount of \$
- A duplicate of this transmittal is attached.

*NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 CFR 1.22(b).*

#### 15. Authorization to Charge Additional Fees

**WARNING:** If no fees are to be paid on filing, the following items should not be completed.

**WARNING:** Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.

- ☒ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 12-0425.
  - ☒ 37 CFR 1.16(a), (f) or (g) (filing fees)
  - ☐ 37 CFR 1.16(b), (c) and (d) (presentation of extra claims)

*NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 CFR 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.*

- ☐ 37 CFR 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)
- ☒ 37 CFR 1.17 (application processing fees)

**WARNING:** While 37 CFR 1.17(a), (b), (c) and (d) deal with extensions of time under §1.136(a), this authorization should be made only with the knowledge that: "Submission of the appropriate extension fee under 37 C.F.R. 1.136(a) is to no avail unless a request or petition for extension is filed." (Emphasis added). Notice of November 5, 1985 (1060 O.G. 27)

- ☒ 37 CFR 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 CFR 1.311(b))

*NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 CFR 1.311(b).*

*NOTE: 37 CFR 1.28(b) requires "Notification of any change in loss of entitlement to small entity status must be filed in the application ... prior to paying, or at the time of paying, ... issue fee". From the wording of 37 CFR 1.28(b): (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.*

**16. Instructions As To Overpayment**

- ☒ credit Account No. 12-0425  
☐ refund



(Signature of attorney)

WILLIAM R. EVANS  
LADAS & PARRY  
26 WEST 61<sup>ST</sup> STREET  
NEW YORK, NEW YORK 10023

Reg. No. 25,858

Tel. No. (212)708-1930

☒ **Incorporation by reference of added pages**

*(Check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)*

- ☐ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added \_\_\_\_

- ☐ Plus Added Pages for Papers Referred to in Item 4 Above

Number of pages added \_\_\_\_

- ☒ Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added 4

☐ **Statement Where No Further Pages Added**

*(If no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item:)*

- ☐ This transmittal ends with this page.

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application: YOUNGDONG WU, et al

For: REMOTE AUTHENTICATION BASED ON EXCHANGING SIGNALS  
REPRESENTING BIOMETRICS INFORMATION

Attorney Docket No.: U 012638-5

**Assistant Commissioner for Patents**  
**Washington, D.C. 20231**

Sir:

**PRELIMINARY AMENDMENT**

Please amend the above application as follows:

**IN THE CLAIMS**

Claim 5, line 1, delete "or 3"

Claim 12, line 1, delete "or 10"

Claim 19, line 1, delete "or 17"

Respectfully submitted,



WILLIAM R. EVANS  
LADAS & PARRY  
26 WEST 61<sup>ST</sup> STREET  
NEW YORK, NEW YORK 10023  
REG.NO.25858(212)708-1930

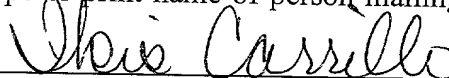
---

**CERTIFICATE UNDER 37 1.10**

I hereby certify that this paper is being deposited with the United States Postal Service on this date MARCH 3, 2000 in an envelope as "EXPRESS MAIL POST OFFICE TO ADDRESS-EE" Mailing Label Number EL386267783US addressed to the: Commissioner of Patents and Trademarks, Washington, D.C. 20231

IBIS CARRILLO

(Type or print name of person mailing paper)



(Signature of person mailing paper)

**NOTE:** Each paper or fee referred to as enclosed herein has the number of the "EXPRESS MAIL" mailing label place thereon prior to mailing 37 CFR 1.16(b).



-1-

## REMOTE AUTHENTICATION BASED ON EXCHANGING SIGNALS REPRESENTING BIOMETRICS INFORMATION

### FIELD OF THE INVENTION

- 5 The present invention relates to the field of secure communications and in particular to techniques of remote authentication of, and secret key establishment between, communicating parties to protect or secure communications over insecure channels.

### BACKGROUND

- 10 Individuals or computer systems often need to have authenticated and confidential communications over an open channels, such as the Internet. While such secure communications may be achieved by physical means, it is more cost effective and flexible to use cryptographic means.
- 15 To have secure communications using cryptographic means, parties need to first execute a protocol to authenticate each other and at the same time establish a mutually agreed conventional up on secret key, which is then used to encrypt subsequent communications between the parties. Conventional authentication and key exchange protocols normally require that, the parties either share a secret (e.g., a password) or
- 20 know each other's public keys.

- A cryptographic system, or cryptosystem, uses an encryption key to convert plaintext into ciphertext (an unintelligible or undecipherable form of the original information) and a decryption key to recover the plaintext from ciphertext. If the encryption key
- 25 and the decryption key are identical, the cryptosystem is referred to as symmetric key cryptosystem. If the encryption and decryption keys are different and it is computationally infeasible to determine the decryption key from the encryption key, the cryptosystem is referred to as an asymmetric key cryptosystem or public key cryptosystem. In a public key cryptosystem, anyone can encrypt a message using a
- 30 public encryption key. However, only the holder of a corresponding private decryption key can decrypt the ciphertext and recover the message.

In a public key cryptosystem, it is often important to securely bind a public key with the legitimate user's ID. Such a binding can be achieved using public key certificates, which are digitally signed and issued by a certification authority.

5 Roughly speaking, a one-way hash function  $h()$  has the properties that:

- 1) for any message  $m$ , the hash  $h(m)$  can be easily computed;
- 2) given  $h(m)$ , finding  $m$  is computationally infeasible; and
- 3) finding two messages that have the same hash is computationally infeasible.

- 10 For more information on cryptosystems, digital signature schemes, public key certificates, and one-way hash functions, reference is made to A. Menezes, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, pp. 425-488, pp. 559-561, and pp. 321-383 1996; and C. Kaufman, R. Perlman, and M. Speciner, Network Security – Private Communication in A Public World, PTR
- 15 Prentice Hall, Englewood Cliffs, NJ, pp. 152-158, pp. 177-204 and pp. 101-129 1995.

- The UNIX (a trademark of Bell Laboratories) operating system provides a classical example of a password based authentication system. In UNIX, each user is provided with a unique login user name and is allowed to choose a secret password. The UNIX
- 20 system maintains a password file containing the user name and a hash of the user's password computed using a one-way hash function with the user's password as input. When a UNIX user desires to access the UNIX system, the user keys in his or her user name and password to a terminal. The terminal computes the hash of the password and sends the hash along with the user name to the UNIX system. Because only the
- 25 user knows the password, if the hash and user name match those in the password file, the user is considered authenticated.

- The UNIX password system is simple to implement, but has a number of problems. Firstly, it is vulnerable to a "replay" attack. That is an eavesdropper can intercept the
- 30 user name and the hash of the password, and replay them to the UNIX system. Secondly, knowing the hash of a password, an eavesdropper can mount an off-line

dictionary attack. The person can guess a password, compute its hash, and see if the two hash values match. The person can then systematically try passwords, one at a time, until a match is found. Since people tend to choose easy to remember or “weak passwords”, such an attack can be very effective. Thirdly, the UNIX system only authenticates the user, and no secret key is established to encrypt subsequent interactions between the user and the system.

A number of authentication and key establishment protocols have been proposed to improve upon the UNIX password protocol. Examples include:

- 1) R. Needham and M. Schroeder, “Using encryption for authentication in large networks of computers”, *Communications of the ACM*, Vol. 21, December 1978, pp. 993-999;
- 2) D. Otway and O. Rees, “Efficient and timely authentication”, *Operating Systems Review*, Vol. 21, No. 1, January 1987, pp. 8-10;
- 3) L. Gong, M. Lomas, R. Needham, and J. Saltzer, “Protecting poorly chosen secrets from guessing attacks”, *IEEE Journal on Selected Areas of Communications*, Vol. 11, No. 5, June 1993, pp. 648-656; and
- 4) US Patent No. 5,440,635 issued to S. Bellovin and M. Merritt on August 8, 1995.

A number of the conventional authentication protocols require that the parties share secret information (such as a password) or possess each other’s public keys in advance. There are many potential difficulties for a human user to share secrets with a large number of remote parties. Firstly, it requires a secure secret distribution mechanism to be in place. Secondly and more importantly, human users are not good at remembering secrets of good quality, since such secrets look like random data. Knowing each other’s public key in authenticated manners is also problematic in a distributed and open environment.

Without good authentication and encryption, voice-over-IP (the Internet protocol) can be eavesdropped without much difficulty. Pretty Good Privacy Phone or PGPfone

(both are trademarks of Pretty Good Privacy Inc.) implements an authentication protocol based on exchange of voice signals and Diffie-Hellman key exchange protocol, P. Zimmermann, *PGPfone Owner's Manual, Version 1.0 beta 5*, 5 January 1996, <http://web.mit.edu/network/pgpfone/manual>.

5

Before proceeding with a discussion of the PGPfone authentication protocol, the Diffie-Hellman key exchange protocol, W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, November 1976 is reviewed. Diffie-Hellman key exchange allows two parties,

10

without sharing keying material in advance, to agree to a secret key over an open channel, but without authentication. In Diffie-Hellman key exchange, two parties A and B agree on an appropriate prime  $p$  and a generator of  $Z_p^*$ , where  $Z_p^* = \{x \mid 0 < x \leq p-1\}$ . Party A generates a random number  $x$ ,  $1 < x < p-1$ , and then computes and sends to Bob  $g^x$  modulo  $p$ . Party B generates a random number  $y$ ,  $1 < y < p-1$ , and

15

then computes and sends to party A  $g^y$  modulo  $p$ .

Party A computes a shared key  $k = (g^y)^x$  modulo  $p$ , and party B computes  $k = (g^x)^y$  modulo  $p$ . The Diffie-Hellman protocol can be carried out in any group in which the discrete logarithm problem is difficult to solve. This protocol, however, is vulnerable to "man-in-the-middle" attacks. If a party C comes in the middle between parties A and B, when party A wishes to have a Diffie-Hellman exchange with party B, party C intercepts all the messages from A and B and enters the Diffie-Hellman exchange with A and B, respectively. As a result, C agrees a secret key with A and another secret key with B so that C can decrypt all the messages from A using the key shared with A and

20

re-encrypt the messages using the key shared with B.

25

The PGPfone authentication protocol assumes that the two parties are familiar with each other's voice. The two parties first establish a shared value (e.g.,  $g^{xy} \bmod p$ ) by performing a Diffie-Hellman exchange. The parties next compute the hash of the shared value. Each party then reads the first few bytes (in hexadecimal format or in

30

English words. PGPfone; maintains a list that maps the 256 values of a byte to 256

English words) of the hash to each other. If the bytes at the two ends match and if the voice sounds like that of the claimed party, the parties are considered authentic.

However, if an attacker is able to collect sound samples of all the 256 words by, for example, eavesdropping on someone's phone calls, the attacker is able to impersonate  
5 the victim at will.

Thus, a need clearly exists for a method of remote authentication based on exchanging signals representing biometrics information and establishing a cryptographic key.

## 10 SUMMARY

In accordance with one aspect of the invention, a method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel. The method includes the steps of:

generating a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed  
15 time interval;

generating a random number  $x$ , computing  $g^x$  modulo  $p$ , where  $g$  and  $p$  are numbers, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , encrypting the first challenge signal with  $k_A$  and a symmetric key cryptosystem, and sending a first ciphertext to the remote party;

20 receiving a second ciphertext from the remote party, sending  $g^x$  modulo  $p$  to the remote party, and starting a clock;

receiving a third ciphertext and  $g^y$  modulo  $p$  from the remote party, stopping the clock, and computing an elapsed time interval of the clock;

deriving a key  $k_B$  from  $g^y$  modulo  $p$ , computing  $g^{xy}$  modulo  $p$ , deriving a key  
25  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , decrypting the second ciphertext with  $k_B$  to recover a second challenge signal from the remote party, decrypting the third ciphertext to recover a first response signal from the remote party;

verifying that the elapsed time of the clock is within a predetermined interval ( $TL_A$ ,  $TU_A$ ), where  $TL_A$  and  $TU_A$  are positive numbers;

30 verifying that the second challenge signal is produced by the remote party;

producing a second response signal of minimum duration  $T$ , encrypting the second response signal with  $k_{AB}$  and sending a fourth ciphertext to the remote party; verifying that the first response signal is a response produced by the remote party to the first challenge signal; and

5        generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

Correspondingly, an apparatus and a computer program product based on the foregoing method are also disclosed.

10

In accordance with another aspect of the invention, there is disclosed a method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel. The method includes the steps of:

15

receiving a first ciphertext from the remote party, generating a random number  $y$ , computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;

producing a first challenge signal of a minimum duration  $T$ , where  $T$  is a fixed time interval;

20

deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting the first challenge signal with  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext to the remote party;

receiving  $g^x$  modulo  $p$  from the remote party, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , decrypting the first ciphertext to recover a second challenge signal from the remote party;

25

verifying that the second challenge signal is produced by the remote party, producing a first response signal of the minimum duration  $T$ ;

computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting the first response signal, sending a third ciphertext and  $g^y$  modulo  $p$  to the remote party, and starting a clock;

receiving a fourth ciphertext, stopping the clock, computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from the remote party;

verifying that the elapsed time of the clock is within a predetermined interval  
5 (TL<sub>B</sub>, TU<sub>B</sub>), where TL<sub>B</sub> and TU<sub>B</sub> are positive numbers;

verifying that the second response signal is a response produced by the remote party to the first challenge signal; and

generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

10

Correspondingly, an apparatus and a computer program product based on the foregoing method are also disclosed.

In accordance with yet another aspect of the invention, there is disclosed a  
15 method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel. The method includes the steps of:

generating a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

20 generating a random number  $x$ , computing  $g^x$  modulo  $p$ , where  $g$  and  $p$  are numbers, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , encrypting the first challenge signal with  $k_A$  and a symmetric key cryptosystem, and sending a first ciphertext to the remote party;

receiving a second ciphertext, sending  $g^x$  modulo  $p$  to the remote party, and  
25 starting a clock;

receiving  $g^y$  modulo  $p$ , computing a key  $k_B$  from  $g^y$  modulo  $p$ , decrypting the second ciphertext to recover a second challenge signal from the remote party;

verifying the second challenge statement to ensure that the second challenge statement is produced by the remote party, and producing a first response signal of  
30 minimum duration  $T$ ;

computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting the first response signal and sending a third ciphertext to the remote party;

receiving a fourth ciphertext from the remote party, stopping the clock, decrypting the fourth ciphertext with  $k_{AB}$  to recover a second response signal from the remote party;

verifying that the elapsed time of the clock is within a predetermined interval  $(tl_A, tu_A)$ , where  $tl_A$  and  $tu_A$  are positive numbers;

verifying that the second response signal is a response produced by the remote party to the first challenge signal; and

generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

Correspondingly, an apparatus and a computer program product based on the foregoing method are also disclosed.

In accordance with a further aspect of the invention, there is disclosed a method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel. The method includes the steps of:

receiving a first ciphertext from remote party, generating a random number  $y$ , and computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;

producing a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting the first challenge signal with  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext;

receiving  $g^x$  modulo  $p$ , computing a key  $k_A$  from  $g^x$  modulo  $p$ , decrypting the first ciphertext to recover a second challenge signal from remote party, sending  $g^y$  to remote party and starting a clock;

verifying the second challenge statement to make sure that the second challenge statement is produced by the remote party, and then producing a first response signal of minimum duration  $T$ ;



computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting the first response signal and sending a third ciphertext to the remote party;

receiving a fourth ciphertext from the remote party, stopping the clock, decrypting the fourth ciphertext with  $k_{AB}$  to recover a second response signal from the remote party;

verifying that the elapsed time of the clock is within an interval  $(tl_B, tu_B)$ , where  $tl_B$  and  $tu_B$  are positive numbers;

verifying that the second response signal is a response produced by the remote party to the first challenge signal; and

generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

Correspondingly, an apparatus and a computer program product based on the foregoing method are also disclosed.

#### BRIEF DESCRIPTION OF THE DRAWINGS

A small number of embodiments of the invention are described hereinafter with reference to the drawings, in which:

- Fig. 1 is a block diagram illustrating a communication system model between two remote individuals over an open transmission channel;
- Fig. 2 is a flowchart depicting the operation of a first embodiment of the invention;
- Fig. 3 is a flowchart showing the operation of a second embodiment of the invention;
- Fig. 4 is a flowchart depicting the first scenario of a man-in-the-middle attack in the first embodiment of Fig. 2;
- Fig. 5 is a flowchart showing the second scenario of a man-in-the-middle attack in the first embodiment of the invention of Fig. 2;
- Fig. 6 is a block diagram illustrating a communication device in accordance with the first embodiment of the invention; and
- Fig. 7 is a block diagram of a general-purpose computer with which the embodiments of the invention can be practised.

## DETAILED DESCRIPTION

A method, an apparatus, and a computer program product for remote authentication based on exchanging signals representing biometrics information and establishing a cryptographic key are described. In the following description, numerous details are set forth including communications channels for example. It will be apparent to one skilled in the art, however, that the present invention may be practised without these specific details. In other instances, well-known features are not described in detail so as not to obscure the present invention.

10

The detailed description is organised as follows:

1. Notation and Definitions
2. Block Diagram of Communications Device
3. First Embodiment
- 15 4. Second Embodiment
5. Security Considerations
6. Computer Implementation

In the following description, components of the system are described as modules. A module, and in particular its functionality, can be implemented in either hardware or software. In the software sense, a module is a process, program, or portion thereof, that usually performs a particular function or related functions. In the hardware sense, a module is a functional hardware unit designed for use with other components or modules. For example, a module may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as an Application Specific Integrated Circuit (ASIC). Numerous other possibilities exist. Those skilled in the art will appreciate that the system can also be implemented as a combination of hardware and software modules.

30

### 1. Notation and Definitions

The following notation is used throughout:

- 5       $A, B$  :      Parties (Alice and Bob, respectively) that seek to have secure communications;
- $e(k, m)$  :      Encrypted message containing original message  $m$  and a key  $k$  using a symmetric key cryptosystem;
- 10       $d(k, c)$  :      Decrypted message containing a ciphertext  $c$  and the key  $k$  using a symmetric key cryptosystem;
- $C_X$  :      An acoustic wave or digital representation of a challenge statement spoken by a party  $X$  (either  $A$  or  $B$ ); whether  $C_X$  is an acoustic wave or a digital representation should be clear to those skilled in the art from the discussion context;
- 15       $R_Y$  :      An acoustic wave or digital representation of a response statement spoken by a party  $Y$  in reply to  $C_X$ ; whether  $R_Y$  is an acoustic wave or a digital representation should be clear to those skilled in the art from the discussion context;
- $|C_X|$  :      the time duration of  $C_X$ ;
- $|R_Y|$  :      the time duration of  $R_Y$ ; and
- 20       $T$  :      A required minimum time duration of any statement spoken by a party.

In the following description, “secure communications” means communications that are authenticated or confidential.

25      Fig. 1 illustrates a general model 100 of communications between two remote individuals. In this model 100, Alice 110 and Bob 150 are two individuals, who are familiar with each other’s biometrics characteristics (without loss of generality, voice signals are used hereinafter) and wish to have a secure communication. The transmission channel 130 represents the means, and more specifically the media, through which communication messages are exchanged between the communication devices 120, 140. The transmission channel 130 includes, but is not limited to, any

30      communications means or media such as computer networks, public telephone

switching networks, and radio links. Alice 110 and Bob 150 communicate with each other by interfacing through communication devices (A) 120 and (B) 140, respectively. Devices (A, B) 120, 140 have appropriate speech signal processing capabilities (such as speech encoding and decoding). The devices 120, 140 accept  
5 audio input, either directly or indirectly, from Alice 110 and Bob 140, respectively, and output the other party's received audio signal.

In the embodiments of the invention, devices (A, B) 120, 140 each exchange signals using a Diffie-Hellman key exchange system and a symmetric key cryptosystem. For  
10 the purposes of illustration only, both devices (A, B) 120, 140 are assumed to have access to a common set of Diffie-Hellman parameters,  $g$  and  $p$ , which may be distributed either off-line or on-line.

The minimum duration of any statement spoken by a party 110, 150 is required to be  
15  $T$ , where  $T$  is either pre-fixed or agreed upon by Alice 110 and Bob 150. For security reasons,  $T$  should be much longer than the channel round-trip delay and the processing delay of each device 120, 140. For example,  $T$  may be in the range of tens of seconds to several minutes, while channel round-trip delay and processing delays are normally less than one second. To keep notation compact, only residues modulo are used  
20 hereinafter: that is,  $g^x$  modulo  $p$ ,  $g^y$  modulo  $p$ , and  $g^{xy}$  modulo  $p$  are written simply as  $g^x$ ,  $g^y$ , and  $g^{xy}$ , respectively. In addition, while not mentioned explicitly, devices (A and B) 110, 150 are assumed to perform audio encoding/decoding and audio compression/decompression operations, whenever necessary.

25 In the embodiments of the invention, the communicating parties are assumed to be familiar with each other's voice (biometrics characteristics in general) and able to recognise each other by listening to each other's speech. This is a reasonable requirement, since there are generally no confidential topics between two strangers without the involvement of a trusted third party. In the embodiments, party 110  
30 (Alice) starts a session with party 150 (Bob) by speaking a challenge statement such as:

“This is Alice! The time is 21 minutes passed 9AM. How was your mid-term examination, Bob?”.

Upon hearing Alice’s message, party 150 (Bob) is expected to speak a response  
5 statement like:

“Hi, Alice! Bob’s here. My mid-term exam was not very good. But thank God, it is over!”.

In the embodiments, Alice is assumed to be able to distinguish whether the stated  
10 response is in Bob’s voice and whether the stated response corresponds to her challenge statement in the first place. Furthermore, it is assumed that it is difficult for an attacker to mimic a target party’s voice to produce a meaningful response statement in real-time.

15 2. Block Diagram of Communications Device

Fig. 6 is a block diagram of a communication device 600 in accordance with the embodiments of the invention. The communications device 600 includes a speech encoding/decoding module 632, a control module 636, an encryption/decryption module 640, a key generator 650, a Diffie Hellman key exchange system 660, a timer module 670, an input/output (I/O) module 680 for transmitting and receiving data via  
20 the communications channel 610, and a memory 682. Optionally, the device 600 also includes a transducer module 630 and an audio compression/decompression module 634.

25 The control module 636 controls the components of the device 600 via signals 690A – 690I. The transducer module 630 converts audio 620 into audio signals and vice versa. Operation of the transducer module 630 can be controlled by the control module 636 via a control signal(s) 690A. In turn, the transducer 630 is coupled bidirectionally with the speech encoding/decoding module 632. This module 632  
30 speech encodes and decodes data and is controlled by the control module 636 via the signal(s) 690B. Optionally, the speech encoding/decoding module 632 is coupled

bidirectionally to an audio compression/decompression module 634. Otherwise, the module 632 can be directly coupled to an encryption/decryption module 640. The control module 636 is coupled to the audio compression/decompression module 634 via the control signal 690C.

5

The encryption/decryption module 640 is optionally coupled to the audio compression/decompression module 634 and is coupled to the control module 636 via a control signal(s) 690D. The encryption/decryption module 640 is also coupled to memory 682, Diffie Hellman key exchange system 660, timer module 670, and the I/O module 680 by bus 692. The key generator 650 is coupled between the Diffie Hellman key exchange system 660 and the encryption/decryption module 640. The key generator 650 produces a key  $k$  from a code  $G^Z$  and is coupled to the control module 636 via a control signal(s) 690E. The memory 682 is coupled to the control module 636 via a control signal(s) 690G.

10

15

The Diffie Hellman key exchange system 660 has as inputs code  $G$ , prime number  $P$ , random value  $X$ , and a control signal(s) 690F from control module 636. The timer module 670 has an interrupt (INT) output to the I/O module 680 that allows the timer module 670 to interrupt transmission/reception of data via the I/O module 680. The timer module 670 is coupled to the control module 636 via a control signal 690I. The I/O module 680 is coupled to the control module 636 by control signal(s) 690H. Operation of the communication device 600 is described hereinafter with reference to the first and second embodiments.

20

25

The embodiments of the invention advantageously employ mechanisms that enable users to authenticate each other and have secure communications over open or insecure channels by using a different technique. More particularly, users are not required to share or remember any secret key or password, or possess each other's public keys in advance. Authentication and key establishment are achieved by exchanging signals representing a remote party's biometrics information. In this connection, the embodiments of the invention utilize a cryptographic one-way hash

30

function. The embodiments concentrate on authenticating remote human users based on the interaction of signals representing a remote party's biometrics information (such as acoustics waves). Parties are assumed to be able to identify each other based on the exchanged biometrics signals. There is no need for the parties to share any  
5 secret key, or know each other's public key in advance. The embodiments of the invention can be advantageously employed in applications such as Internet telephoning or voice-over-IP (Internet Protocol).

### 3. First Embodiment

10 Fig. 2 is a flowchart illustrating the method of secure communications according to the first embodiment of the invention. The flowchart is organised in columns in the following order: Alice 110, device (A) 120, device (B) 140, and Bob 150. In step 210, Alice 110 speaks a challenge statement  $C_A$ , which is input to Device A (shown as device 600 in Fig. 6). Preferably, the challenge statement  $C_A$  contains some  
15 "freshness" elements, such as the date and time, and news headlines of the day. In step 212, Device A generates a random number  $x$  and computes  $g^x$ . Device A then preferably computes a key  $k_A$  from code  $g^x$  using the key generator. Next, Device A encrypts the challenge statement  $C_A$  with key  $k_A$  using the key generator and sends the ciphertext, referred to as Message A1:

20 
$$e(k_A, C_A),$$

preferably together with Alice's identity to Device B over the transmission channel 610.

In step 214, Device B receives the Message A1 and prompts Bob to speak a challenge  
25 statement  $C_B$  in step 216. In step 218, Device B generates a random number  $y$ , computes  $g^y$  and preferably a key  $k_B$  from the code  $g^y$  for a symmetric key cryptosystem. Device B then encrypts  $C_B$  and transmits the ciphertext, referred to as Message A2:

$$e(k_B, C_B),$$

30 preferably together with Bob's identity to Device A.

In step 220, Device A receives the Message A2. In step 222, Device A sends to Device B the code, referred to as Message A3:

$$g^x,$$

and starts a clock or timer to measure the time interval for a response. In step 224,  
5 after receiving code  $g^x$ , Device B computes the key  $k_A$  from the code  $g^x$  and decrypts the ciphertext received in Message A1 to recover the challenge statement  $C_A$ . Device B then plays back the challenge statement  $C_A$  to Bob. In step 226, Bob listens to the challenge statement  $C_A$  and verifies that the voice belongs to Alice. If the verification fails, Bob terminates the session. Otherwise, in step 228, Bob speaks a response  
10 statement  $R_B$  in reply to the challenge statement  $C_A$  (e.g., by iterating  $C_A$  in his own voice).

In step 230, Device B computes the code  $(g^x)^y = g^{xy}$  and a key  $k_{AB}$  from  $g^{xy}$  in well-known fashion for the symmetric key cryptosystem, and encrypts  $R_B$  with  $k_{AB}$  and the  
15 symmetric key cryptosystem to obtain  $e(k_{AB}, R_B)$ . In step 232, Device B sends, as Message A4, the following:

$$g^y, e(k_{AB}, R_B),$$

to Device A and then starts its clock.

20 In step 234, upon receipt of Message A4, Device A first stops its clock started in step 222. Time  $t_A$  is the elapsed time of the clock. Device A then computes the code  $(g^y)^x = g^{yx}$ , the key  $k_{AB}$  from code  $g^{yx}$ , and the key  $k_B$  from the code  $g^y$ . Device A then decrypts  $e(k_B, C_B)$  with the key  $k_B$  and  $e(k_{AB}, R_B)$  with key  $k_{AB}$  to recover the challenge statement  $C_B$  and the response  $R_B$ , respectively.  $|C_A|$  is the duration of the  
25 challenge statement  $C_A$ , and  $|R_B|$  is the duration of the response  $R_B$ . It will be readily apparent to those skilled in the art how to obtain the duration of an audio signal. Let  $TL_A = |C_A| + |R_B|$ . Further, in step 230, Device A checks the elapsed time  $t_A$  to see if:

$$t_A \in (TL_A, TU_A), \quad (1)$$

where  $TU_A$  can be taken advantageously as  $T + TL_A$  if the channel round trip delay  
30 and processing delay in Devices A and B 120, 140 are negligible compared with  $T$ . Such delays can be easily incorporated into Equation (1) by those skilled in the art. If



$t_A \in (TL_A, TU_A)$  is not true, Device A terminates the session. Otherwise, in step 236, Alice listens and verifies the challenge statement  $C_B$ .

If Alice recognises that the challenge statement  $C_B$  is not Bob's voice, Alice

- 5 terminates the session. Otherwise, in step 238, Alice speaks a response statement  $R_A$  (e.g., by iterating  $C_B$  in her own voice) in reply to the challenge statement  $C_B$ . In step 240, Device A encrypts the response statement  $R_A$  with the key  $k_{AB}$  and sends to Device B the ciphertext, as Message A5:

$$e(k_{AB}, R_A).$$

- 10 In step 248, following step 238, Alice listens and verifies the response statement  $R_B$ . If the response statement  $R_B$  is not either a response to the challenge statement  $C_A$  or in Bob's voice, Alice stops the session. If Alice is sure that the response statement  $R_B$  is a reply to the challenge statement  $C_A$  in Bob's voice, she begins communicating in step 250.

15

Next, from step 240 in step 242, upon receipt of Message A5, Device B stops its clock or timer. The time  $t_B$  is the elapsed time of the clock. Also, Device B decrypts  $e(k_{AB}, R_A)$  with the key  $k_{AB}$  to obtain the response statement  $R_A$ . Let  $|C_B|$  denotes the playback duration of  $C_B$  and  $|R_A|$  the playback duration of  $R_A$ . Let  $TL_B = |C_B| + |R_A|$ .

- 20 In step 242, Device B checks the elapsed time to see if:

$$t_B \in (TL_B, TU_B), \quad (2)$$

where  $TU_B$  can be taken advantageously as  $T + TL_B$  if the channel round trip delay and processing delay at Devices A and B are negligible in comparison with  $T$ . If

Equation (2) is not satisfied, Device B terminates the session. Otherwise, Device B

- 25 plays back the response statement  $R_A$  to Bob. In step 244, Bob listens and verifies the response statement  $R_A$ . If Bob recognises that  $R_A$  is a reply to the challenge statement  $C_B$  in Alice's voice, Bob can be confident that he is communicating with Alice and he can proceed to step 246. Otherwise, Bob stops the session.

- 30 In steps 250 and 246, respectively, Bob and Alice preferably communicate with each other. In step 252, Device A encrypts messages from Alice and decrypts messages

from Bob with a key derived from  $g^{xy}$ , preferably using another symmetric key cryptosystem. Similarly, in step 256, Device B likewise encrypts messages from Bob and decrypts message from Alice with a key derived from  $g^{xy}$  in the same way as Device A and with the same symmetric key cryptosystem as used by Device A.

5

#### 4. Second Embodiment

Fig. 3 is a flowchart illustrating a method of secure communications according to the second embodiment of the invention. In step 310, Alice starts the session by speaking a challenge statement  $C_A$ . In step 312, Device A generates a random value  $x$ ,  
10 computes a code  $g^x$  and a key  $k_A$  from  $g^x$  for a symmetric key cryptosystem, encrypts the challenge statement  $C_A$  with  $k_A$  and sends to B the ciphertext, as Message B1:

$$e(k_A, C_A).$$

In step 314, Device B receives Message B1. Next, in step 316, Device B prompts Bob  
15 to speak a challenge statement  $C_B$  in step 318. In step 316, Device B then generates a random number  $y$ , computes code  $g^y$  and a key  $k_B$  from  $g^y$  for a symmetric key cryptosystem, encrypts  $C_B$  with  $k_B$  and sends to Alice the ciphertext, as message B2:

$$e(k_B, C_B).$$

20 In step 320, Device A receives Message B2. Next, in step 322, Device A sends to Bob, as Message B3:

$$g^x,$$

and starts a clock.

25 In step 324, upon receipt of the Message B3, Device B computes a key  $k_A$  from code  $g^x$ , decrypts  $e(k_A, C_A)$  to recover  $C_A$ , sends to Alice as Message B4:

$$g^y,$$

and starts a clock. Device B then outputs the challenge statement  $C_A$  to Bob. In step 326, Bob listens and verifies whether the challenge statement  $C_A$  is in Alice's voice.

30 Bob terminates the process if he has doubts on the originality of the challenge statement  $C_A$ . When the challenge statement  $C_A$  is verified successfully by Bob, in

step 328, Bob speaks a response statement  $R_B$  in reply to the challenge statement  $C_A$ . In step 330, Device B computes code  $g^{xy}$  and a key  $k_{AB}$  from  $g^{xy}$ , encrypts  $R_B$  and sends to Alice the ciphertext, as Message B5:

$e(k_{AB}, R_B)$ .

5

On the other hand, Message B4 is received by Device A in step 332. Device A computes  $k_B$  from  $g^y$ , decrypts  $e(k_B, C_B)$  to recover  $C_B$ . Alice listens and verifies  $C_B$  in step 334. Alice stops the process if she believes that  $C_B$  is not in Bob's voice;

otherwise, she speaks a response statement  $R_A$  in reply to  $C_B$  in step 336. In step 338,

10 Device A computes  $g^{yx}$  and  $k_{AB}$  from  $g^{yx}$ , encrypts  $R_A$  and sends to Bob the ciphertext, as Message B6:

$e(k_{AB}, R_A)$ .

In step 340, Device A receives Message B5. Device A also stops the clock, decrypts  
15  $e(k_{AB}, R_B)$  to recover the response statement  $R_B$  and checks to see if the elapsed time of the clock  $T_A$  satisfies the following:

$$T_A \in (tl_A, tu_A), \quad (3)$$

where preferably  $tl_A = |C_A| + |R_B|$  and  $tu_A = tl_A + T$ . Device A terminates the session if Equation (3) is not satisfied. Otherwise, Device A outputs the response statement

20  $R_B$  to Alice. In step 342, Alice listens and verifies the response statement  $R_B$ . Alice stops the session if she is not convinced that the response statement  $R_B$  is Bob's response to the challenge statement  $C_A$ . Otherwise, in step 344, Alice starts communications with Bob.

25 In step 348, upon receipt of the Message B6, Device B stops its clock, decrypts  $e(k_{AB}, R_A)$  to recover  $R_A$ . Device B, then checks to see if the elapsed time of its clock satisfies the following:

$$T_B \in (tl_B, tu_B) \quad (4)$$

where preferably  $tl_B = |C_B| + |R_A|$  and  $tu_B = tl_B + T$ . Device B terminates the session if

30 Equation (4) is not satisfied. Otherwise, Device B outputs the response statement  $R_A$  to Bob. In step 350, Bob listens and verifies  $R_A$ . Bob stops the session if he is not

convinced that the response statement  $R_A$  is Alice's response to  $C_B$ . Otherwise, in step 352, he starts communications with Alice.

With successful authentication of both Alice and Bob, Devices A and B, derive a key  
5 from  $g^{xy}$  and use the key to encrypt and decrypt messages between Alice and Bob in steps 346 and 354, respectively, using communications obtained in steps 344 and 352.

### 5. Security Considerations

Symmetric key cryptosystems are used in the embodiments to encrypt challenge  
10 signals and response signals. It is important that all encryptions resist data modification (such as cut and paste) attacks.

The symmetric key cryptosystem used to encrypt challenge and response signals can be replaced by a cryptographic commitment function. Such a commitment function  
15 has the following properties:

- 1) no one can modify the contents of the commitment without being detected; and
- 2) no one can get any information about its contents unless the committing party discloses the information.

20

One way to form a commitment function is using a cryptographic one-way hash function  $h()$ . To commit to an item  $I$ , the committing party computes the commitment  $h(k \parallel I)$ , where  $k$  is a secret key and  $k \parallel I$  is the concatenation of  $k$  and  $I$ . To verify the commitment, the verifying party must have  $k$  and  $I$ , compute  $h(k \parallel I)$  and compare  $h$   
25  $(k \parallel I)$  with the commitment.

Checking the lengths of the elapsed time intervals of the clocks in both illustrative embodiments is very important in detecting any man-in-the-middle attacks. This is illustrated using the two attacking scenarios respectively, in relation to the first  
30 embodiment of Fig. 2. A similar analysis can be done for the second embodiment. In the following descriptions, the term "Alice" is used to refer to both the user Alice and

Device A. Similarly, the term “Bob” is used to denote both the user Bob and Device B.

Fig. 4 depicts a scenario where Alice attempts to set up a communications session with Bob and where Clark performs a man-in-the-middle attempt to impersonate Bob to Alice. The flow diagram is accordingly organised into three columns: Alice, Clark and Bob. In step 410, Alice starts a session by generating a random number  $x$ , computing  $g^x$ , speaking a challenge statement  $C_A$ , computing  $k_A$  from  $g^x$ , encrypting  $C_A$  with  $k_A$ , and sending the ciphertext  $e(k_A, C_A)$  to Bob.

In step 412, the ciphertext is intercepted by Clark. Clark generates a number  $z$ , computes  $g^z$  and a key  $k_C$  from  $g^z$ , encrypts an old challenge statement  $C'_B$  from Bob, and sends the ciphertext  $e(k_C, C'_B)$  to Alice. In step 414, Alice receives the ciphertext, replies with  $g^x$  and starts a clock. The code  $g^x$  is again intercepted by Clark at step 416. In step 416, Clark derives the key  $k_A$  from  $g^x$  and decrypts  $e(k_A, C_A)$  to recover  $C_A$ . Clark cannot mimic Bob’s voice to produce a meaningful response statement  $R_B$ , so Clark impersonates Alice and starts a new session with Bob by sending Bob  $e(k_C, C_A)$ .

In step 418, upon receipt of  $e(k_C, C_A)$ , Bob generates a random value  $y$ , and computes code  $g^y$  and a key  $k_B$ . Bob then speaks a challenge statement  $C_B$ , encrypts the challenge statement using key  $k_B$ , and sends the ciphertext  $e(k_B, C_B)$  to Alice. Clark intercepts the ciphertext in step 420. To continue impersonating Alice, Clark sends  $g^z$  to Bob. In step 422, Bob computes key  $k_C$  from  $g^z$ , decrypts  $e(k_C, C_A)$ , and listens  $C_A$ , which was indeed spoken by Alice. Bob speaks a response statement  $R_B$ , computes a key  $k_{BC}$  from  $g^{zy}$ , encrypts  $R_B$  with  $k_{BC}$ , and transmits  $g^y$  and the ciphertext  $e(k_{BC}, R_B)$ . In step 424, Clark again intercepts the ciphertext, computes the key  $k_{BC}$  from  $g^{yz}$ , and decrypts  $e(k_{BC}, R_B)$ . Now Clark gets  $R_B$ . Clark then computes  $k_{AC}$  from  $g^{xz}$ , encrypts  $R_B$  with  $k_{AC}$ , and sends the ciphertext  $e(k_{AC}, R_B)$  to Alice.

In step 426, Alice stops the clock, decrypts  $e(k_C, C'_B)$  and  $e(k_{AC}, R_B)$  to recover  $C'_B$  and  $R_B$ , respectively. Alice also listens and verifies that  $C'_B$  is in Bob's voice. Alice then speaks and encrypts a response statement  $R_A$ , and sends the ciphertext  $e(k_{AC}, R_A)$ .

- 5 Next, in step 428, Alice listens and verifies the response statement  $R_B$ . Since  $R_B$  is indeed a response to  $C_A$  from Bob, Alice is fooled into believing Clark is Bob. However, the embodiments of the invention prevent this from happening by checking the clock's elapsed time  $t_A$  against the interval  $(TL_A, TU_A)$  per Equation (1), where  $TL_A = |C_A| + |R_B|$ , and  $TU_A = TL_A + T$ .

10

To appreciate the rationale behind Equation (1), without the man-in-the-middle attack by Clark,  $t_A = |C_A| + |R_B| + \Delta_{A1}$ , where  $\Delta_{A1}$  is the delay due to processing, transmission, and a pause interval introduced by Bob after listening to the challenge statement  $C_A$ , but before speaking the response statement  $R_B$ . However, with the man-in-the-middle attack shown in Fig. 4,  $t_A = |C_A| + |R_B| + |C_B| + \Delta_{A2}$ , where  $\Delta_{A2}$  is a delay similar to  $\Delta_{A1}$ . Since it is required that  $T \gg \Delta_{A1}$  and  $\Delta_{A2}$  and that  $|C_B| \leq T$ . It can be readily appreciated that  $t_A = |C_A| + |R_B| + |C_B| + \Delta_{A2} > TL_A + T = TU_A$  with the attack and that  $t_A = |C_A| + |R_B| + \Delta_{A1} \approx TL_A < TU_A$  without the attack. Therefore, by checking  $t_A$  against Equation (1), the man-in-the-middle attacked can be detected.

20

Fig. 5 shows a second scenario 500 of a man-in-the-middle attack, where Clark impersonates Alice to Bob. Again the flow diagram is organised in columns: Alice, Clark, and Bob. In step 510, Clark generates  $z$ , computes  $g^z$  and a key  $k_C$  from  $g^z$ , and encrypts  $C'_A$  – an old statement from Alice. Clark starts the impersonation by sending the ciphertext  $e(k_C, C'_A)$  to Bob.

25

In step 512, upon receipt of the message from Clark, Bob generates  $y$ ,  $g^y$ , and a key  $k_B$  from  $g^y$ . Bob then speaks a challenge statement  $C_B$ , encrypts the challenge statement with  $k_B$ , and transmits the ciphertext  $e(k_B, C_B)$  to Alice. In step 514, the ciphertext is intercepted by Clark and Clark sends  $g^z$  to Bob. In step 516, Bob derives the key  $k_C$  from  $g^z$ , and decrypts  $e(k_C, C'_A)$  with  $k_C$  to recover  $C'_A$ . Bob listens to the challenge

30

statement  $C'_A$  and believes that  $C'_A$  was indeed spoken by Alice. Bob then speaks a response statement  $R_B$ , derives a key  $k_{BC}$  from  $g^{zy}$ , encrypts  $R_B$ , transmits the ciphertext  $e(k_{BC}, R_B)$  and  $g^y$  and starts a clock.

- 5 Next, in step 518, upon interception of the ciphertext  $e(k_{BC}, R_B)$  and  $g^y$ , Clark derives  $k_B$  from  $g^y$  and  $k_{BC}$  from  $g^{zy}$ , and decrypts  $e(k_B, C_B)$  to recover  $C_B$ . Since Clark is not able to reply to the challenge statement  $C_B$  in Alice's voice, Clark encrypts the challenge  $C_B$  with  $k_C$  and starts a session with Alice by sending  $e(k_C, C_B)$  to Alice. In step 520, upon receipt of  $e(k_C, C_B)$ , Alice generates  $x$ ,  $g^x$ , and a key  $k_A$  from  $g^x$ . Alice
- 10 then speaks a challenge statement  $C_A$ , encrypts the challenge statement with  $k_A$ , and sends the ciphertext  $e(k_A, C_A)$ . In step 522, Clark intercepts the ciphertext and sends  $g^z$  to Alice. In step 524, Alice derives a key  $k_{AC}$  from  $g^{zx}$ , and decrypts  $e(k_C, C_B)$  to recover  $C_B$ . Alice then listens to the challenge statement  $C_B$  and believes that she hears Bob's voice. Alice then speaks a response statement  $R_A$ , encrypts the response
- 15 statement with  $k_{AC}$  and sends  $g^x$  and the ciphertext  $e(k_{AC}, R_A)$ . In step 526, Clark intercepts the message from Alice and decrypts the ciphertext to obtain the response  $R_A$ . Clark then encrypts the response statement with  $k_{BC}$  and sends the ciphertext  $e(k_{BC}, R_A)$  to Bob.
- 20 In step 528, Bob receives  $e(k_{BC}, R_A)$ , stops the clock, and decrypts the ciphertext to recover  $R_A$ . Without checking the elapsed time of the clock,  $t_B$ , Bob can be misled into believing that Bob is communication with Alice since  $R_A$  is Alice's reply to the challenge statement  $C_B$ . This attack can be foiled easily by checking  $t_B$  against the interval  $(TL_B, TU_B)$  (see Equation 2), where  $TL_B = |C_B| + |R_A|$  and  $TU_B = TL_B + T$ .
- 25 Without the man-in-the-middle attack by Clark,  $t_B = |C_B| + |R_A| + \Delta_{B1}$ , where  $\Delta_{B1}$  is the delay due to processing, transmission, and a pause interval introduced by Alice after listening to  $C_B$  but before speaking the response statement  $R_A$ . With the man-in-the-middle attack of Fig. 5,  $t_B = |C_B| + |R_A| + |C_A| + \Delta_{B2}$ , where  $\Delta_{B2}$  is a delay similar to  $\Delta_{B1}$ . It is required that  $T \gg \Delta_{B1}$  and  $\Delta_{B2}$  and that  $|C_A| \leq T$ . Then it can be seen that  $t_B =$
- 30  $|C_B| + |R_A| + |C_A| + \Delta_{B2} < TL_B + T = TU_B$  with the attack and  $t_B = |C_B| + |R_A| + \Delta_{B1} \approx$

$TL_B < TU_B$  without the attack. Therefore, by checking  $t_B$  against Equation (2), the man-in-the-middle attack can be detected.

#### 6. Computer Implementation

- 5 The embodiments of the invention are preferably implemented using a computer(s), such as the general-purpose computer shown in Fig. 7. In particular, the processes of Figs. 2 and 3 can be implemented as software, or a computer program, executing on the computer, where each communication device 120, 140, 600 of Figs. 1 and 6 can be implemented using a general purpose computer. The method or process steps for
- 10 remote authentication based on exchanging signals representing biometrics information are effected by instructions in the software that are carried out by the computer. The software may be implemented as one or more modules for implementing the process steps. A module is a part of a computer program that usually performs a particular function or related functions. Also, as described
- 15 hereinbefore, a module can also be a packaged functional hardware unit for use with other components or modules.

- In particular, the software may be stored in a computer readable medium, including the storage devices described below. The software is preferably loaded into the
- 20 computer from the computer readable medium and then carried out by the computer. A computer program product includes a computer readable medium having such software or a computer program recorded on it that can be carried out by a computer. The use of the computer program product in the computer preferably effects an advantageous apparatus for remote authentication based on exchanging signals
- 25 representing biometrics information in accordance with the embodiments of the invention.

- The computer system 700 consists of the computer 702, a video display 716, and input devices 718, 720. In addition, the computer system 700 can have any of a number of
- 30 other output devices including line printers, laser printers, plotters, and other reproduction devices connected to the computer 702. The computer system 700 can



be connected to one or more other computers via a communication interface 708b using an appropriate communication channel 730 such as a modem communications path, a computer network, or the like. The computer network may include a local area network (LAN), a wide area network (WAN), an Intranet, and/or the Internet.

5

The computer 702 itself consists of a central processing unit(s) (simply referred to as a processor hereinafter) 704, a memory 706 which may include random access memory (RAM) and read-only memory (ROM), input/output (IO) interfaces 708A, & 708B a video interface 710, and one or more storage devices generally represented by a block  
10 712 in Fig. 8. The storage device(s) 712 can consist of one or more of the following: a floppy disc, a hard disc drive, a magneto-optical disc drive, CD-ROM, magnetic tape or any other of a number of non-volatile storage devices well known to those skilled in the art. Each of the components 704 to 712 is typically connected to one or more of the other devices via a bus 714 that in turn can consist of data, address, and  
15 control buses.

The video interface 710 is connected to the video display 716 and provides video signals from the computer 702 for display on the video display 716. User input to operate the computer 702 can be provided by one or more input devices 708B. For  
20 example, an operator can use the keyboard 718 and/or a pointing device such as the mouse 720 to provide input to the computer 702.

The system 700 is simply provided for illustrative purposes and other configurations can be employed without departing from the scope and spirit of the invention.  
25 Computers with which the embodiment can be practiced include IBM-PC/ATs or compatibles, one of the Macintosh <sup>TM</sup> family of PCs, Sun Sparcstation <sup>TM</sup>, a workstation or the like. The foregoing are merely exemplary of the types of computers with which the embodiments of the invention may be practiced. Typically, the processes of the embodiments, described hereinafter, are resident as software or a  
30 program recorded on a hard disk drive (generally depicted as block 712 in Fig. 7) as the computer readable medium, and read and controlled using the processor 704.

Intermediate storage of the program and pixel data and any data fetched from the network may be accomplished using the semiconductor memory 706, possibly in concert with the hard disk drive 712.

- 5 In some instances, the program may be supplied to the user encoded on a CD-ROM or a floppy disk (both generally depicted by block 712), or alternatively could be read by the user from the network via a modem device connected to the computer, for example. Still further, the software can also be loaded into the computer system 700 from other computer readable medium including magnetic tape, a ROM or integrated circuit, a magneto-optical disk, a radio or infra-red transmission channel between the  
10 computer and another device, a computer readable card such as a PCMCIA card, and the Internet and Intranets including email transmissions and information recorded on websites and the like. The foregoing are merely exemplary of relevant computer readable mediums. Other computer readable mediums may be practiced without departing from the scope and spirit of the invention.  
15

Thus, a method, an apparatus, and a computer program product for remote authentication based on exchanging signals representing biometrics information and establishing a cryptographic key have been described. While only a small number of  
20 embodiments are described, it will be apparent to those skilled in the art, in view of this disclosure, that numerous changes and/or modifications can be made without departing from the scope and spirit of the invention.

-27-

## CLAIMS

1. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:
  - 5 generating a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;
    - generating a random number  $x$ , computing  $g^x$  modulo  $p$ , where  $g$  and  $p$  are numbers, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , encrypting said first challenge signal with  $k_A$  and a symmetric key cryptosystem, and sending a first ciphertext to said
    - 10 remote party;
      - receiving a second ciphertext from said remote party, sending  $g^x$  modulo  $p$  to said remote party, and starting a clock;
      - receiving a third ciphertext and  $g^y$  modulo  $p$  from said remote party, stopping the clock, and computing an elapsed time interval of said clock;
      - 15 deriving a key  $k_B$  from  $g^y$  modulo  $p$ , computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , decrypting said second ciphertext with  $k_B$  to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;
        - verifying that said elapsed time of the clock is within a predetermined interval
        - 20  $(TL_A, TU_A)$ , where  $TL_A$  and  $TU_A$  are positive numbers;
          - verifying that said second challenge signal is produced by said remote party;
          - producing a second response signal of minimum duration  $T$ , encrypting said second response signal with  $k_{AB}$  and sending a fourth ciphertext to said remote party;
          - verifying that said first response signal is a response produced by said remote
          - 25 party to said first challenge signal; and
            - generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with said remote party.
    2. The method according to claim 1, wherein  $T$  is larger than the channel
    - 30 transmission and processing delay.

3. The method according to claim 1, wherein said challenge signals and response signals represent biometrics characteristics of the producing parties.

4. The method according to claim 3, wherein said biometrics characteristics include the voice of a person.

5. The method according to claim 1 or 3, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics.

6. The method according to claim 1, wherein encryption of said challenge and response signals is performed using a cryptographic commitment function.

7. The method according to claim 1, where  $TL_A$  is  $t_1 + t_2$  and  $TU_A$  is  $t_1 + t_2 + T$ , with  $t_1$  being the duration of said first challenge signal and  $t_2$  being the duration of said first response signal.

8. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said apparatus including:

means for generating a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

means for generating a random number  $x$ , computing  $g^x$  modulo  $p$ , where  $g$  and  $p$  are numbers, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , encrypting said first challenge signal with  $k_A$  and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

means for receiving a second ciphertext from said remote party, sending  $g^x$  modulo  $p$  to said remote party, and starting a clock;

means for receiving a third ciphertext and  $g^y$  modulo  $p$  from said remote party, stopping the clock, and computing an elapsed time interval of said clock;

means for deriving a key  $k_B$  from  $g^y$  modulo  $p$ , computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , decrypting said second ciphertext with  $k_B$  to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;

5 means for verifying that said elapsed time of the clock is within a predetermined interval ( $TL_A$ ,  $TU_A$ ), where  $TL_A$  and  $TU_A$  are positive numbers;

means for verifying that said second challenge signal is produced by said remote party;

means for producing a second response signal of minimum duration  $T$ ,  
10 encrypting said second response signal with  $k_{AB}$  and sending a fourth ciphertext to said remote party;

means for verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications  
15 with said remote party.

9. The apparatus according to claim 8, wherein  $T$  is larger than the channel transmission and processing delay.

20 10. The apparatus according to claim 8, wherein said challenge signals and response signals represent biometrics characteristics of the producing parties.

11. The apparatus according to claim 10, wherein said biometrics characteristics include the voice of a person.

25

12. The apparatus according to claim 8 or 10, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics.

13. The apparatus according to claim 8, wherein encryption of said challenge and response signals is performed using a cryptographic commitment function.

5           14. The apparatus according to claim 8, where  $TL_A$  is  $t_1 + t_2$  and  $TU_A$  is  $t_1 + t_2 + T$ , with  $t_1$  being the duration of said first challenge signal and  $t_2$  being the duration of said first response signal.

10           15. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said computer program product including:

computer readable program code means for generating a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

15           computer readable program code means for generating a random number  $x$ , computing  $g^x$  modulo  $p$ , where  $g$  and  $p$  are numbers, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , encrypting said first challenge signal with  $k_A$  and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

20           computer readable program code means for receiving a second ciphertext from said remote party, sending  $g^x$  modulo  $p$  to said remote party, and starting a clock;

computer readable program code means for receiving a third ciphertext and  $g^y$  modulo  $p$  from said remote party, stopping the clock, and computing an elapsed time interval of said clock;

25           computer readable program code means for deriving a key  $k_B$  from  $g^y$  modulo  $p$ , computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , decrypting said second ciphertext with  $k_B$  to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;

30           computer readable program code means for verifying that said elapsed time of the clock is within a predetermined interval ( $TL_A$ ,  $TU_A$ ), where  $TL_A$  and  $TU_A$  are positive numbers;

computer readable program code means for verifying that said second challenge signal is produced by said remote party;

computer readable program code means for producing a second response signal of minimum duration  $T$ , encrypting said second response signal with  $k_{AB}$  and  
5 sending a fourth ciphertext to said remote party;

computer readable program code means for verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

computer readable program code means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with said remote party.

10

16. The computer program product according to claim 15, wherein  $T$  is larger than the channel transmission and processing delay.

17. The computer program product according to claim 15, wherein said  
15 challenge signals and response signals represent biometrics characteristics of the producing parties.

18. The computer program product according to claim 17, wherein said biometrics characteristics include the voice of a person.

20

19. The computer program product according to claim 15 or 17, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics.

25 20. The computer program product according to claim 15, wherein encryption of said challenge and response signals is performed using a cryptographic commitment function.

21. The computer program product according to claim 15, where  $TL_A$  is  $t_1$   
30  $+ t_2$  and  $TU_A$  is  $t_1 + t_2 + T$ , with  $t_1$  being the duration of said first challenge signal and  $t_2$  being the duration of said first response signal.

22. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:

- 5 receiving a first ciphertext from said remote party, generating a random number  $y$ , computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;  
producing a first challenge signal of a minimum duration  $T$ , where  $T$  is a fixed time interval;  
deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting said first challenge signal with  
10  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;  
receiving  $g^x$  modulo  $p$  from said remote party, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , decrypting said first ciphertext to recover a second challenge signal from said remote party;  
15 verifying that said second challenge signal is produced by said remote party, producing a first response signal of said minimum duration  $T$ ;  
computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal, sending a third ciphertext and  $g^y$  modulo  $p$  to said remote party, and starting a clock;  
20 receiving a fourth ciphertext, stopping said clock, computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;  
verifying that said elapsed time of said clock is within a predetermined interval ( $TL_B$ ,  $TU_B$ ), where  $TL_B$  and  $TU_B$  are positive numbers;  
25 verifying that said second response signal is a response produced by said remote party to said first challenge signal; and  
generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

- 30 23. The method according to claim 22, wherein  $T$  is larger than the channel transmission and processing delay



24. The method according to claim 22, wherein said challenge signals and response signals are signals representing biometrics characteristics.

5 25. The method according to claim 22, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity with a remote party's biometrics characteristics.

10 26. The method according to claim 22, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

15 27. The method according to claim 22, wherein  $TL_B$  is  $t_3 + t_4$  and  $TU_B$  is  $t_3 + t_4 + T$ , with  $t_3$  being the duration of the first challenge signal and  $t_4$  being the duration of the second response signal.

28. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said apparatus including:

20 means for receiving a first ciphertext from said remote party, generating a random number  $y$ , computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;

means for producing a first challenge signal of a minimum duration  $T$ , where  $T$  is a fixed time interval;

25 means for deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting said first challenge signal with  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;

means for receiving  $g^x$  modulo  $p$  from said remote party, deriving a key  $k_A$  from and  $g^x$  modulo  $p$ , decrypting said first ciphertext to recover a second challenge signal from said remote party;

30 means for verifying that said second challenge signal is produced by said remote party, producing a first response signal of said minimum duration  $T$ ;

means for computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal, sending a third ciphertext and  $g^y$  modulo  $p$  to said remote party, and starting a clock;

means for receiving a fourth ciphertext, stopping said clock, computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;

means for verifying that said elapsed time of said clock is within a predetermined interval  $(TL_B, TU_B)$ , where  $TL_B$  and  $TU_B$  are positive numbers;

means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

29. The apparatus according to claim 28, wherein  $T$  is larger than the channel transmission and processing delay

30. The apparatus according to claim 28, wherein said challenge signals and response signals are signals representing biometrics characteristics.

31. The apparatus according to claim 28, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity with a remote party's biometrics characteristics.

32. The apparatus according to claim 28, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

33. The apparatus according to claim 28, wherein  $TL_B$  is  $t_3 + t_4$  and  $TU_B$  is  $t_3 + t_4 + T$ , with  $t_3$  being the duration of the first challenge signal and  $t_4$  being the duration of the second response signal.

34. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said computer program product including:

5 computer readable program code means for receiving a first ciphertext from said remote party, generating a random number  $y$ , computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;

computer readable program code means for producing a first challenge signal of a minimum duration  $T$ , where  $T$  is a fixed time interval;

10 computer readable program code means for deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting said first challenge signal with  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;

computer readable program code means for receiving  $g^x$  modulo  $p$  from said remote party, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , decrypting said first ciphertext  
15 to recover a second challenge signal from said remote party;

computer readable program code means for verifying that said second challenge signal is produced by said remote party, producing a first response signal of said minimum duration  $T$ ;

computer readable program code means for computing  $g^{xy}$  modulo  $p$ , deriving  
20 a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal, sending a third ciphertext and  $g^y$  modulo  $p$  to said remote party, and starting a clock;

computer readable program code means for receiving a fourth ciphertext, stopping said clock, computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;

25 computer readable program code means for verifying that said elapsed time of said clock is within a predetermined interval  $(TL_B, TU_B)$ , where  $TL_B$  and  $TU_B$  are positive numbers;

computer readable program code means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

30 computer readable program code means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

35. The computer program product according to claim 34, wherein T is larger than the channel transmission and processing delay

5 36. The computer program product according to claim 34, wherein said challenge signals and response signals are signals representing biometrics characteristics.

10 37. The computer program product according to claim 34, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity with a remote party's biometrics characteristics.

15 38. The computer program product according to claim 34, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

20 39. The computer program product according to claim 34, wherein  $TL_B$  is  $t_3 + t_4$  and  $TU_B$  is  $t_3 + t_4 + T$ , with  $t_3$  being the duration of the first challenge signal and  $t_4$  being the duration of the second response signal.

40. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:

25 generating a first challenge signal of minimum duration T, where T is a fixed time interval;

generating a random number x, computing  $g^x$  modulo p, where g and p are numbers, deriving a key  $k_A$  from  $g^x$  modulo p, encrypting said first challenge signal with  $k_A$  and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

30 receiving a second ciphertext, sending  $g^x$  modulo p to said remote party, and starting a clock;

receiving  $g^y$  modulo  $p$ , computing a key  $k_B$  from  $g^y$  modulo  $p$ , decrypting the second ciphertext to recover a second challenge signal from said remote party;

verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of  
5 minimum duration  $T$ ;

computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal and sending a third ciphertext to said remote party;

receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with  $k_{AB}$  to recover a second response signal from  
10 said remote party;

verifying that said elapsed time of said clock is within a predetermined interval  $(tl_A, tu_A)$ , where  $tl_A$  and  $tu_A$  are positive numbers;

verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

15 generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with said remote party.

41. The method according to claim 40, wherein  $T$  is larger than the channel transmission and processing delay  
20

42. The method according to claim 40, wherein said challenge signals and response signals are signals representing biometrics characteristics.

43. The method according to claims 40, wherein verification of said  
25 second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics.

44. The method according to claim 40, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.  
30

45. The method according to claim 40, where  $tl_A$  is  $T_1 + T_2$  and  $tu_A$  is  $T_1 + T_2 + T$ , with  $T_1$  being the duration of said first challenge signal and  $T_2$  being the duration of said second response signal.

5           46. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said apparatus including:

              means for generating a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

10           means for generating a random number  $x$ , computing  $g^x$  modulo  $p$ , where  $g$  and  $p$  are numbers, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , encrypting said first challenge signal with  $k_A$  and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

              means for receiving a second ciphertext, sending  $g^x$  modulo  $p$  to said remote party, and starting a clock;

15           means for receiving  $g^y$  modulo  $p$ , computing a key  $k_B$  from  $g^y$  modulo  $p$ , decrypting the second ciphertext to recover a second challenge signal from said remote party;

              means for verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of minimum duration  $T$ ;

20           means for computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal and sending a third ciphertext to said remote party;

25           means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with  $k_{AB}$  to recover a second response signal from said remote party;

              means for verifying that said elapsed time of said clock is within a predetermined interval  $(tl_A, tu_A)$ , where  $tl_A$  and  $tu_A$  are positive numbers;

30           means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with said remote party.

47. The apparatus according to claim 46, wherein  $T$  is larger than the  
5 channel transmission and processing delay

48. The apparatus according to claim 46, wherein said challenge signals and response signals are signals representing biometrics characteristics.

49. The apparatus according to claims 46, wherein verification of said  
10 second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics.

50. The apparatus according to claim 46, wherein encryption of said  
15 challenge and response signals is carried out by a cryptographic commitment function.

51. The apparatus according to claim 46, where  $tl_A$  is  $T_1 + T_2$  and  $tu_A$  is  $T_1 + T_2 + T$ , with  $T_1$  being the duration of said first challenge signal and  $T_2$  being the duration of said second response signal.  
20

52. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said computer program product including:

25 computer readable program code means for generating a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

computer readable program code means for generating a random number  $x$ , computing  $g^x$  modulo  $p$ , where  $g$  and  $p$  are numbers, deriving a key  $k_A$  from  $g^x$  modulo  $p$ , encrypting said first challenge signal with  $k_A$  and a symmetric key cryptosystem,  
30 and sending a first ciphertext to said remote party;

computer readable program code means for receiving a second ciphertext, sending  $g^x$  modulo  $p$  to said remote party, and starting a clock;

computer readable program code means for receiving  $g^y$  modulo  $p$ , computing a key  $k_B$  from  $g^y$  modulo  $p$ , decrypting the second ciphertext to recover a second  
5 challenge signal from said remote party;

computer readable program code means for verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of minimum duration  $T$ ;

computer readable program code means for computing  $g^{xy}$  modulo  $p$ , deriving  
10 a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal and sending a third ciphertext to said remote party;

computer readable program code means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with  $k_{AB}$  to recover a second response signal from said remote party;

15 computer readable program code means for verifying that said elapsed time of said clock is within a predetermined interval  $(tl_A, tu_A)$ , where  $tl_A$  and  $tu_A$  are positive numbers;

computer readable program code means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

20 computer readable program code means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with said remote party.

53. The computer program product according to claim 52, wherein  $T$  is larger than the channel transmission and processing delay  
25

54. The computer program product according to claim 52, wherein said challenge signals and response signals are signals representing biometrics characteristics.



55. The computer program product according to claims 52, wherein verification of said second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics.

5 56. The computer program product according to claim 52, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

10 57. The computer program product according to claim 52, where  $tl_A$  is  $T_1 + T_2$  and  $tu_A$  is  $T_1 + T_2 + T$ , with  $T_1$  being the duration of said first challenge signal and  $T_2$  being the duration of said second response signal.

15 58. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:

receiving a first ciphertext from remote party, generating a random number  $y$ , and computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;

producing a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

20 deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting said first challenge signal with  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext;

receiving  $g^x$  modulo  $p$ , computing a key  $k_A$  from  $g^x$  modulo  $p$ , decrypting said first ciphertext to recover a second challenge signal from remote party, sending  $g^y$  to remote party and starting a clock;

25 verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration  $T$ ;

computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal and sending a third ciphertext to said remote party;

receiving a fourth ciphertext from said remote party, stopping said clock,  
decrypting said fourth ciphertext with  $k_{AB}$  to recover a second response signal from  
said remote party;

5        verifying that said elapsed time of the clock is within an interval  $(tl_B, tu_B)$ ,  
      where  $tl_B$  and  $tu_B$  are positive numbers;

      verifying that said second response signal a response produced by said remote  
party to said first challenge signal; and

      generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the  
remote party.

10

59.     The method according to claim 58, wherein  $T$  is larger than the channel  
transmission and processing delay

60.     The method according to claim 58, wherein said challenge signals and  
15    response signals are signals representing biometrics characteristics.

61.     The method according to claim 58, wherein verification of said second  
challenge signal and said second response signal from said remote party is based on  
familiarity of said remote party's biometrics characteristics.

20

62.     The method according to claim 58, wherein encryption of challenge  
and response signals are carried out by a cryptographic commitment function.

63.     The method according to claim 58, where  $tl_B$  is  $T_3 + T_4$  and  $tu_B$  is  $T_3 +$   
25     $T_4 + T$ , with  $T_3$  being the duration of said first challenge signal and  $T_4$  being said  
duration of said second response signal.

64.     An apparatus for authenticating a remote party and establishing a  
cryptographic key for secure communications via an insecure communications  
30    channel, said apparatus:

means for receiving a first ciphertext from remote party, generating a random number  $y$ , and computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;

means for producing a first challenge signal of minimum duration  $T$ , where  $T$  is a fixed time interval;

5 means for deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting said first challenge signal with  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext;

means for receiving  $g^x$  modulo  $p$ , computing a key  $k_A$  from  $g^x$  modulo  $p$ , decrypting said first ciphertext to recover a second challenge signal from remote party, sending  $g^y$  to remote party and starting a clock;

10 means for verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration  $T$ ;

means for computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal and sending a third ciphertext to said remote party;

15 means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting said fourth ciphertext with  $k_{AB}$  to recover a second response signal from said remote party;

means for verifying that said elapsed time of the clock is within an interval  $(tl_B, tu_B)$ , where  $tl_B$  and  $tu_B$  are positive numbers;

20 means for verifying that said second response signal a response produced by said remote party to said first challenge signal; and

means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

25

65. The apparatus according to claim 64, wherein  $T$  is larger than the channel transmission and processing delay

66. The apparatus according to claim 64, wherein said challenge signals and response signals are signals representing biometrics characteristics.

30

67. The apparatus according to claim 64, wherein verification of said second challenge signal and said second response signal from said remote party is based on familiarity of said remote party's biometrics characteristics.

5           67. The apparatus according to claim 64, wherein encryption of challenge and response signals are carried out by a cryptographic commitment function.

68. The apparatus according to claim 64, where  $tl_B$  is  $T_3 + T_4$  and  $tu_B$  is  $T_3 + T_4 + T$ , with  $T_3$  being the duration of said first challenge signal and  $T_4$  being said  
10          duration of said second response signal.

69. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an  
15          insecure communications channel, said computer program product:

computer readable program code means for receiving a first ciphertext from remote party, generating a random number  $y$ , and computing  $g^y$  modulo  $p$ , where  $g$  and  $p$  are numbers;

computer readable program code means for producing a first challenge signal  
20          of minimum duration  $T$ , where  $T$  is a fixed time interval;

computer readable program code means for deriving a key  $k_B$  from  $g^y$  modulo  $p$ , encrypting said first challenge signal with  $k_B$  and a symmetric key cryptosystem, and sending a second ciphertext;

computer readable program code means for receiving  $g^x$  modulo  $p$ , computing  
25          a key  $k_A$  from  $g^x$  modulo  $p$ , decrypting said first ciphertext to recover a second challenge signal from remote party, sending  $g^y$  to remote party and starting a clock;

computer readable program code means for verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration  $T$ ;

computer readable program code means for computing  $g^{xy}$  modulo  $p$ , deriving a key  $k_{AB}$  from  $g^{xy}$  modulo  $p$ , encrypting said first response signal and sending a third ciphertext to said remote party;

5 computer readable program code means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting said fourth ciphertext with  $k_{AB}$  to recover a second response signal from said remote party;

computer readable program code means for verifying that said elapsed time of the clock is within an interval  $(tl_B, tu_B)$ , where  $tl_B$  and  $tu_B$  are positive numbers;

10 computer readable program code means for verifying that said second response signal a response produced by said remote party to said first challenge signal; and

computer readable program code means for generating a key  $k$  from  $g^{xy}$  modulo  $p$  for secure communications with the remote party.

70. The computer program product according to claim 69, wherein  $T$  is  
15 larger than the channel transmission and processing delay

71. The computer program product according to claim 69, wherein said challenge signals and response signals are signals representing biometrics characteristics.  
20

72. The computer program product according to claim 69, wherein verification of said second challenge signal and said second response signal from said remote party is based on familiarity with said remote party's biometrics characteristics.  
25

73. The computer program product according to claim 69, wherein encryption of challenge and response signals are carried out by a cryptographic commitment function.

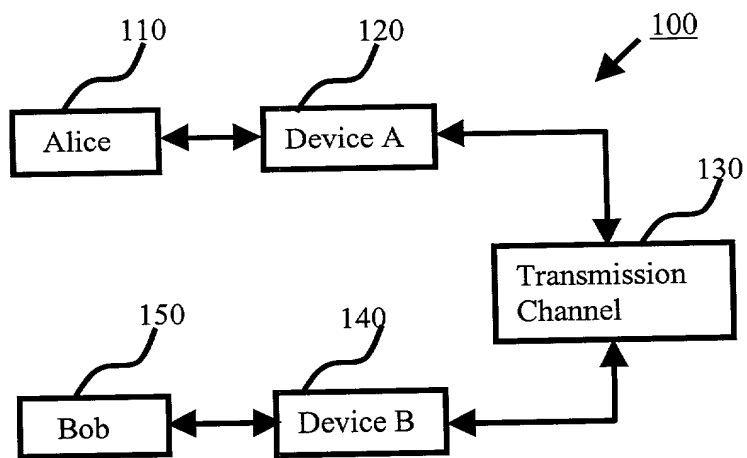
74. The computer program product according to claim 69, where  $tl_B$  is  $T_3 + T_4$  and  $tu_B$  is  $T_3 + T_4 + T$ , with  $T_3$  being the duration of said first challenge signal and  $T_4$  being said duration of said second response signal.

## REMOTE AUTHENTICATION BASED ON EXCHANGING SIGNALS REPRESENTING BIOMETRICS INFORMATION

### 5 ABSTRACT

A method, an apparatus, and a computer program product for remote authentication are disclosed. The methods are based on exchanging of signals representing remote party's biometrics information (such as acoustic waveforms) and have application in secure telephony or video-conferencing communications over open networks. The  
10 apparatus includes a speech encoding/decoding module (632), a control module (636), an encryption/decryption module (640), a key generator (650), a Diffie Hellman key exchange system (660), a timer module (670) for measuring time between a challenged statement and a corresponding response statement, an input/output (I/O) module (680) for transmitting and receiving data via a communications channel 610.

15 FIG. 6



**FIG. 1**



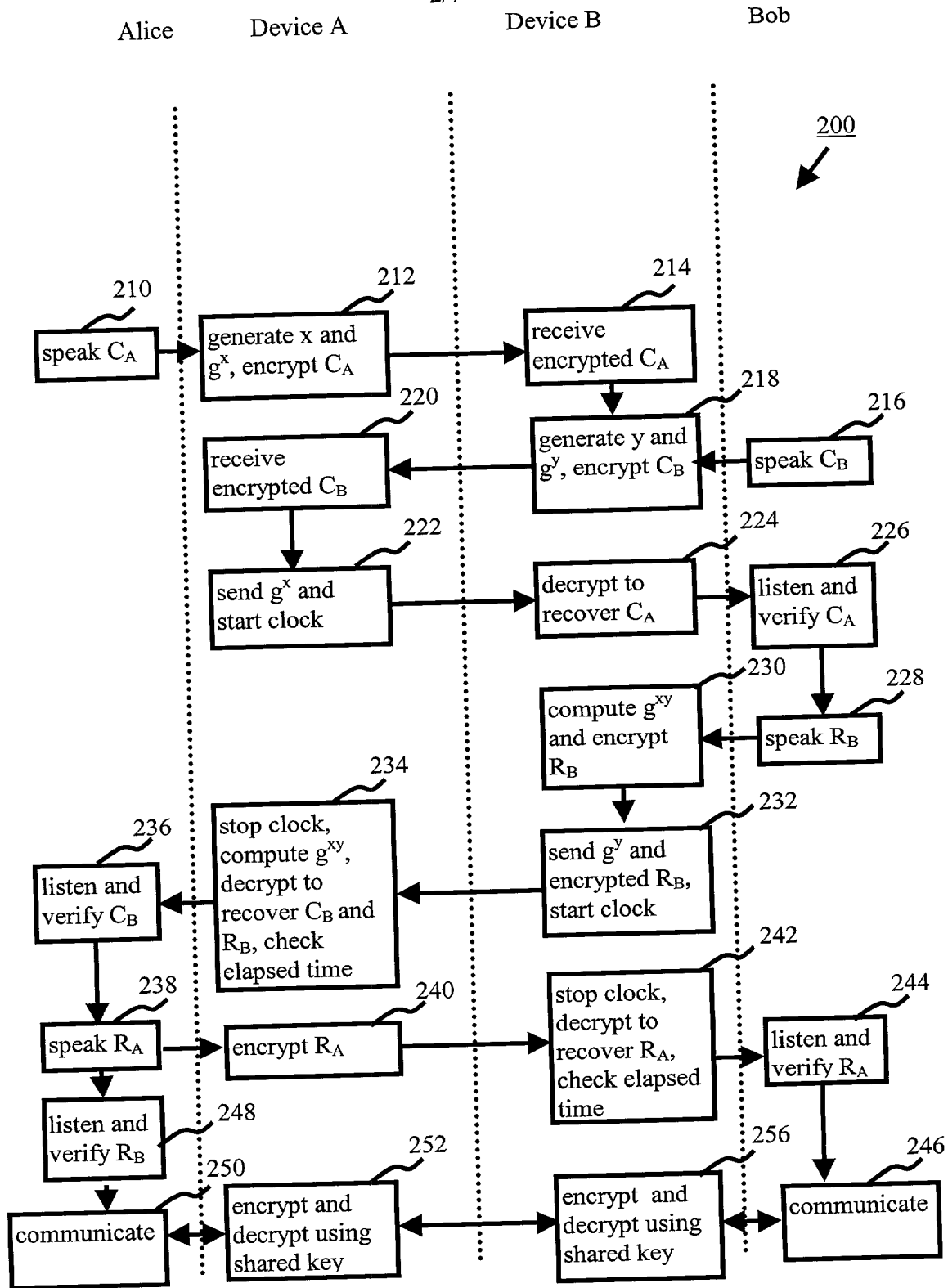


FIG. 2

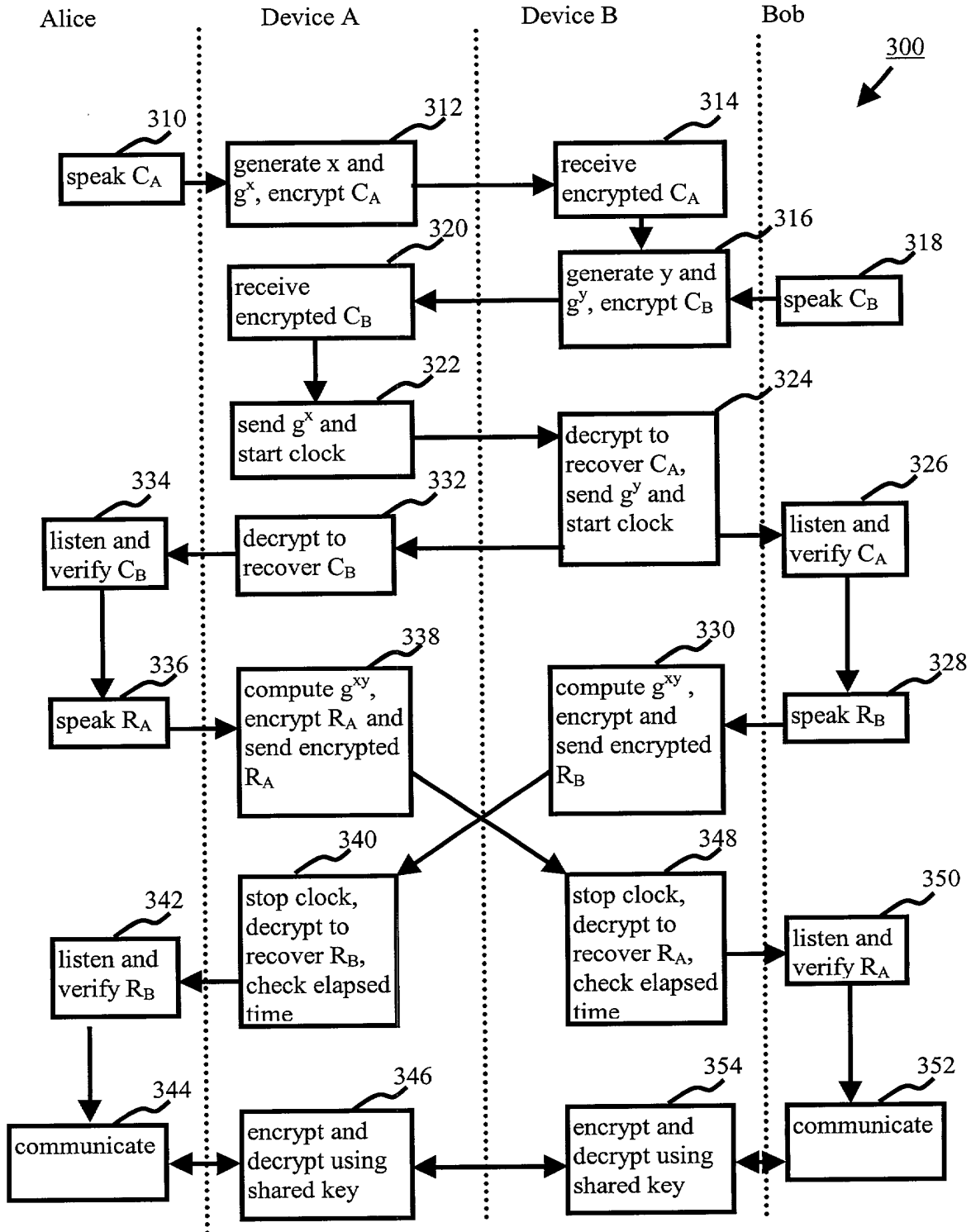


FIG. 3

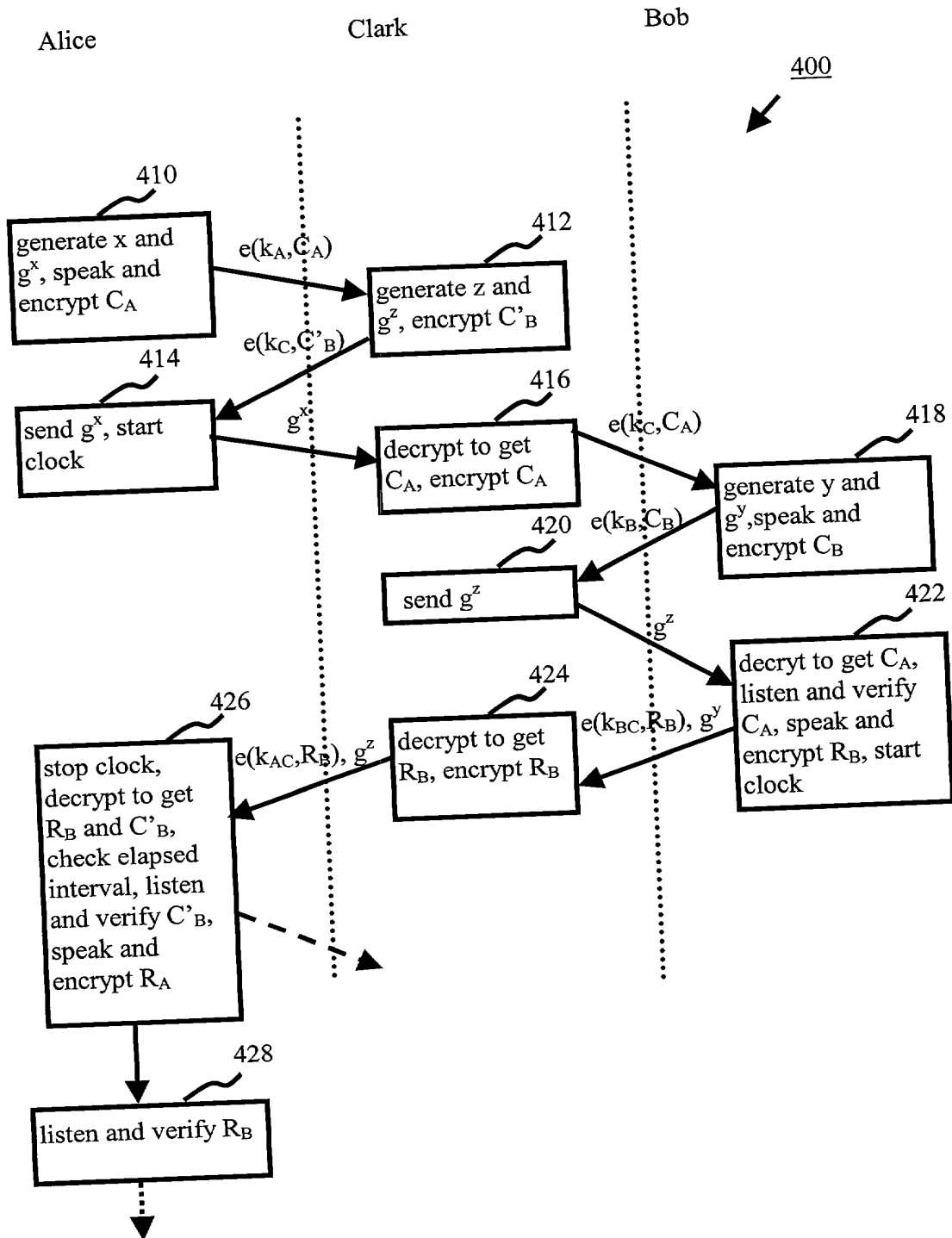


FIG. 4

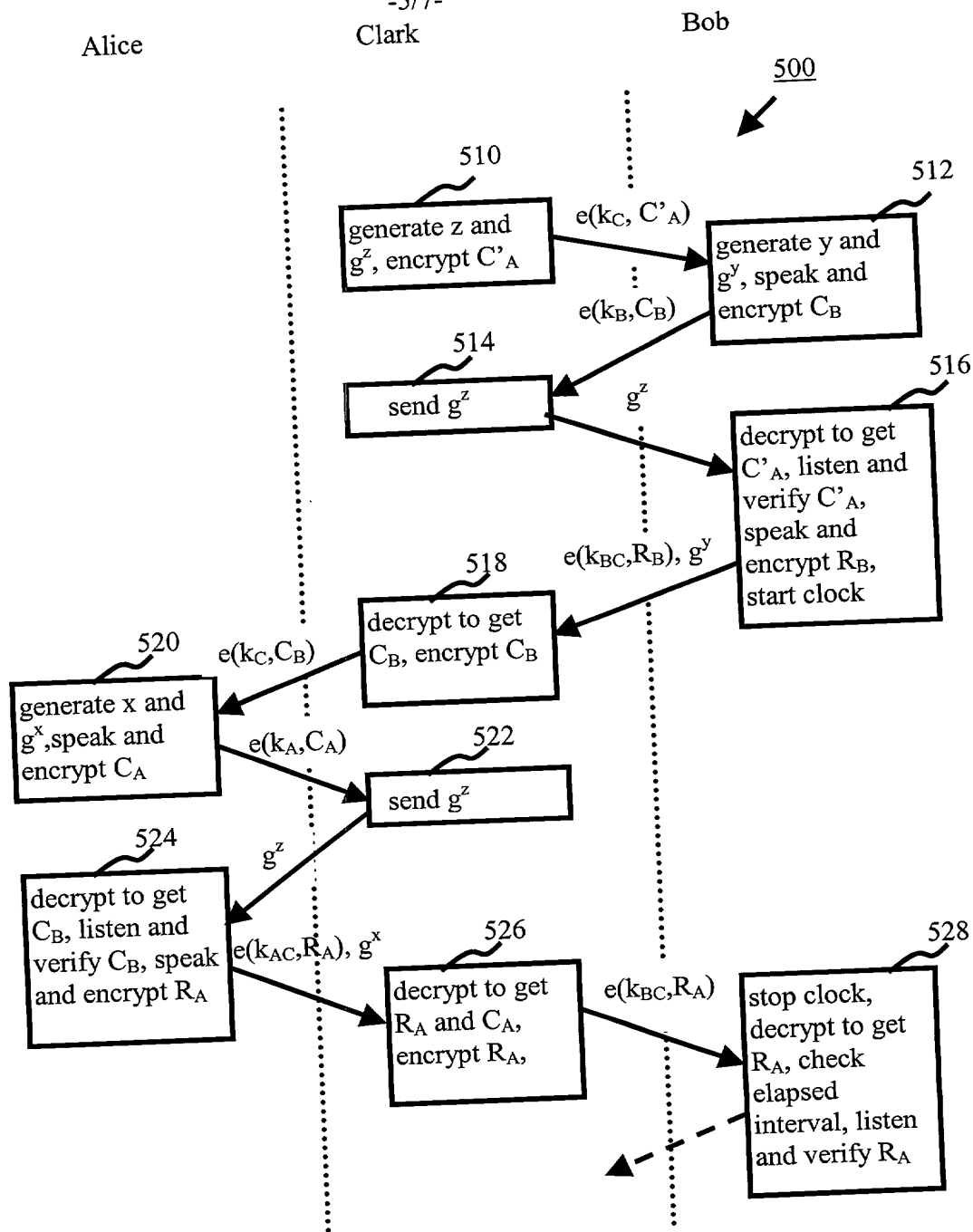
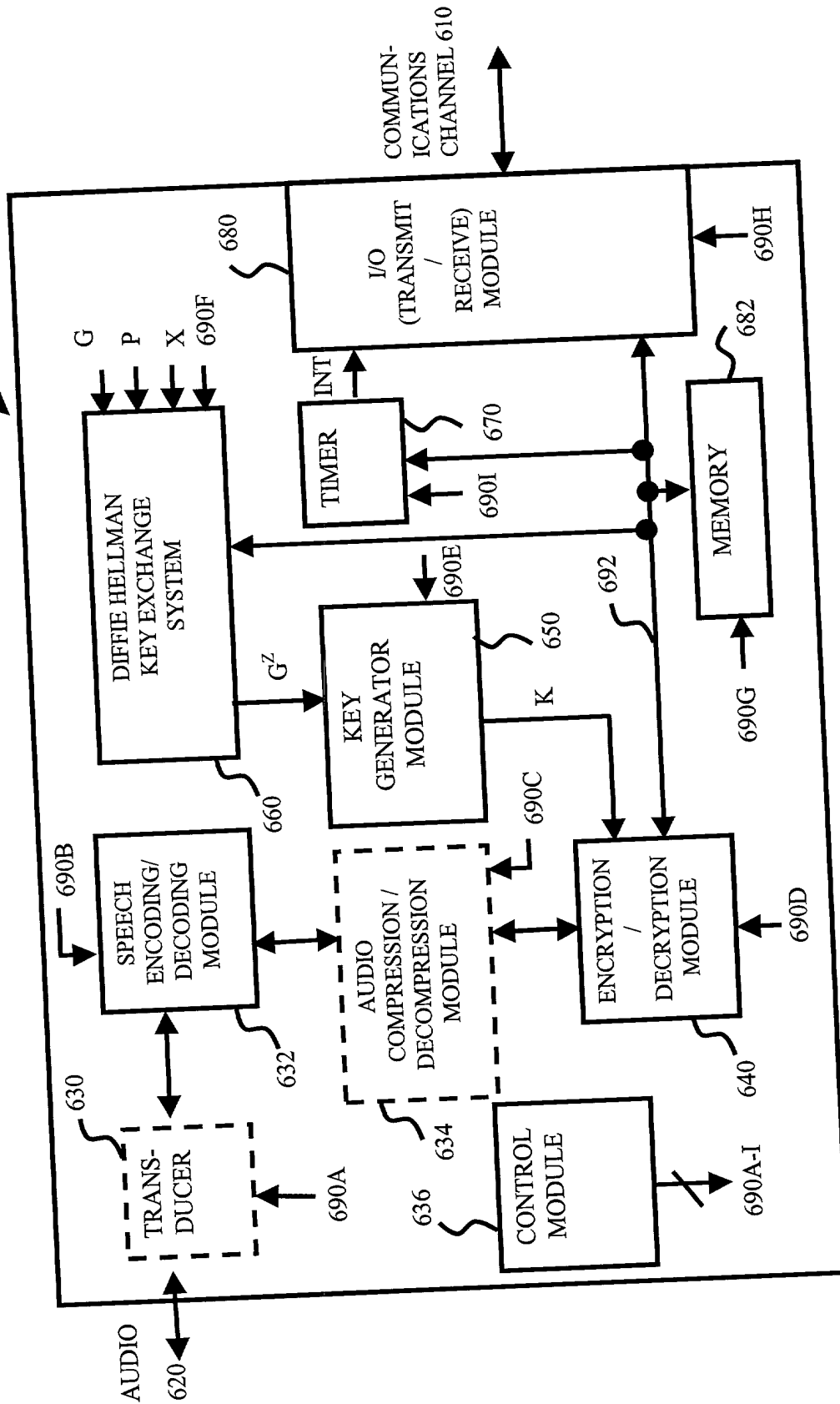


FIG. 5

-6/7-

600



-6/7-

COMMUNICATIONS  
CHANNEL 610

FIG. 6

-7/7-

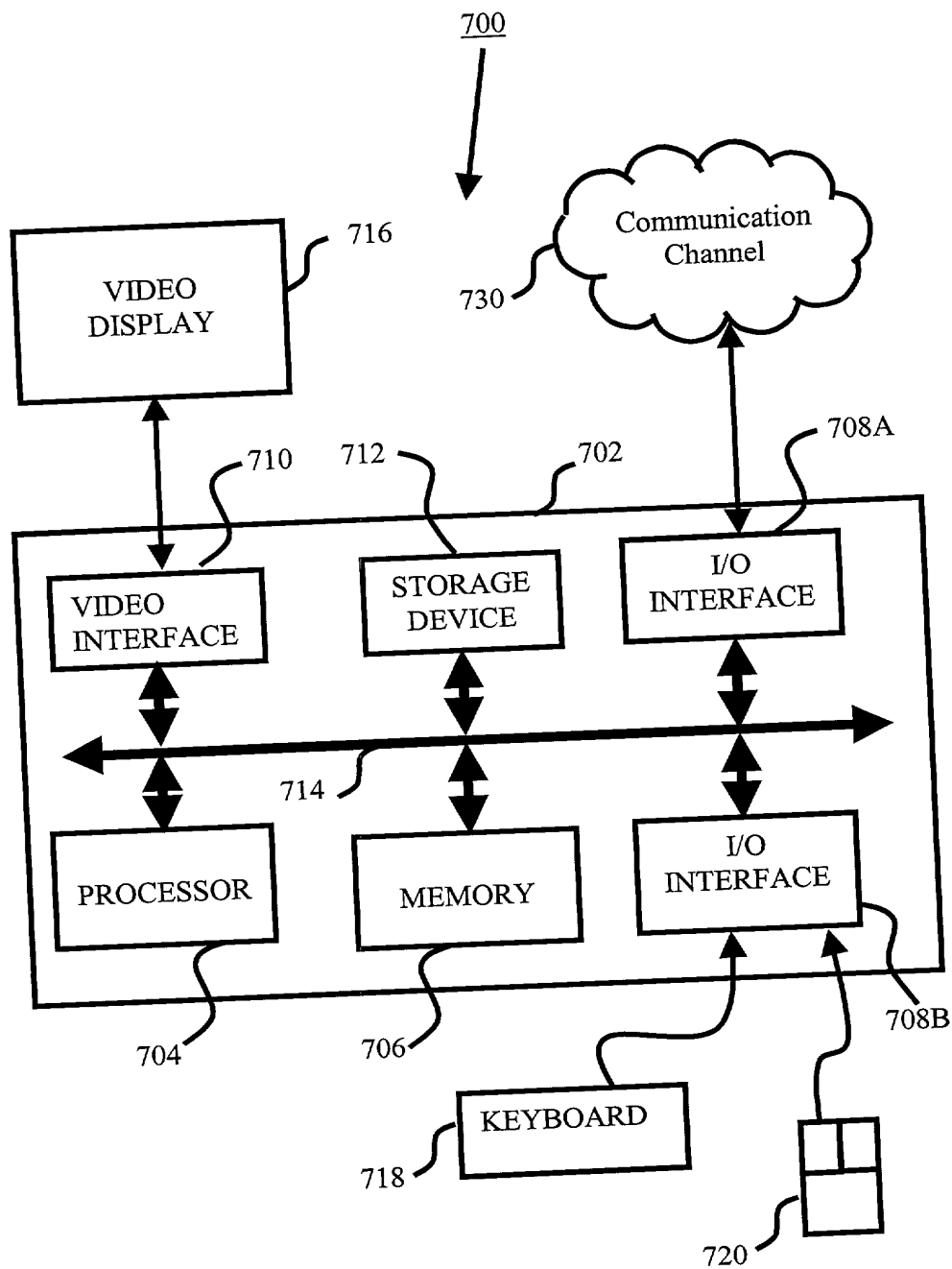


FIG. 7

Please type a plus sign (+) inside this box → ☐

PTO/SB/01 (12-97)  
Approved for use through 9/30/00. OMB 0660-0032

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**DECLARATION FOR UTILITY OR  
DESIGN  
PATENT APPLICATION  
(37 CFR 1.63)**

☒ Declaration Submitted with Initial Filing OR ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number

First Named Inventor

WU, Yongdong

**COMPLETE IF KNOWN**

Application Number

/

Filing Date

Group Art Unit

Examiner Name

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**REMOTE AUTHENTICATION BASED ON EXCHANGING SIGNALS  
REPRESENTING BIOMETRICS INFORMATION**

the specification of which (Title of the Invention)

☒ is attached hereto  
OR

☐ was filed on (MM/DD/YYYY) as United States Application Number or PCT International

Application Number and was amended on (MM/DD/YYYY) (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
9906598-8	SINGAPORE	12/24/1999	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

EXPRESS MAIL LABEL  
NO.: EL386267783US

Please type a plus sign (+) inside this box → ☐

## DECLARATION

ADDITIONAL INVENTOR(S)  
Supplemental Sheet  
Page \_\_\_\_ of \_\_\_\_

Name of Additional Joint Inventor, if any:

☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])

Family Name or Surname

Huijie, Robert

DENG

Inventor's  
Signature

*R. Deng*

Date

24/12/00

Residence: City

State

Country

Singapore

Citizenship

Singapore

Post Office Address

2 Namly Rise

Post Office Address

City

Singapore

State

ZIP

267110

Country

Singapore

Name of Additional Joint Inventor, if any:

☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])

Family Name or Surname

Feng

BAO

Inventor's  
Signature

*W. B. Feng*

Date

24/12/00

Residence: City

Singapore

State

Country

Singapore

Citizenship

China

Post Office Address

37, West Coast Park, #04-06, Park View Condo

Post Office Address

City

Singapore

State

ZIP

127653

Country

Singapore

Name of Additional Joint Inventor, if any:

☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])

Family Name or Surname

Inventor's  
Signature

Date

Residence: City

State

Country

Citizenship

Post Office Address

Post Office Address

City

State

ZIP

Country

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

EXPRESS MAIL LABEL  
NO.: EL386267783US



Please type a plus sign (+) inside this box → ☐

PTO/SB/01 (12-97)  
Approved for use through 9/1/00  
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE  
10106365

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

## DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

☐ Customer Number

OR

☐ Registered practitioner(s) name/registration number listed below

Place Customer  
Number Bar Code  
Label here

Name	Registration Number	Name	Registration Number

☐ Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to: ☐ Customer Number or Bar Code Label ☐ OR ☐ Correspondence address below

Name			
Address			
Address			
City	State	ZIP	
Country	Telephone	Fax	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor:		<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name or Surname	
Yongdong		WU	
Inventor's Signature	Date		
Residence: City	Singapore	State	Country
Post Office Address	10, Ghim Moh Road, #13-80		
Post Office Address			
City	Singapore	State	Country
ZIP	270010	Country	Singapore

☐ Additional inventors are being named on the 1 supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto

EXPRESS MAIL LABEL  
NO.: EL386267783US

Please type a plus sign (+) inside this box ➡ ☐

U 012638-5

Approved for use through 6/30/99. OMB 0651-0035

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**POWER OF ATTORNEY OR  
AUTHORIZATION OF AGENT,  
NOT ACCOMPANYING  
APPLICATION**

Application Number

Filing Date

First Named Inventor

WU, Yongdong

Group Art Unit

Examiner Name

Attorney Docket Number

I hereby appoint:

☐ Practitioners at Customer Number

OR

☒ Practitioner(s) named below:

Place Customer  
Number Bar Code  
Label here

Name	Registration Number
JOSEPH H. HANDLEMAN	26179
JOHN RICHARDS	31053
RICHARD J. STREIT	25765
JULIAN H. COHEN	20302

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

<input checked="" type="checkbox"/> Firm or Individual Name	LADAS & PARRY				
Address	26 WEST 61ST STREET				
Address					
City	NEW YORK	State	NY	ZIP	10023
Country	UNITED STATES OF AMERICA				
Telephone	(212) 708-1800	Fax	(212) 246-8959		

I am the:

☒ Applicant.

☐ Assignee of record of the entire interest  
*Certificate under 37 CFR 3.73(b) is enclosed*

**SIGNATURE of Applicant or Assignee of Record**

Name	WU, Yongdong
Signature	<i>Wu Yongdong</i>
Date	25/02/2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

EXPRESS MAIL LABEL  
NO.: EL386267783US

Please type a plus sign (+) inside this box ➔ ☒

U 012638-5

Approved for use through 6/30/99. OMB 0651-0035

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

**POWER OF ATTORNEY OR  
AUTHORIZATION OF AGENT,  
NOT ACCOMPANYING  
APPLICATION**

Application Number

Filing Date

First Named Inventor

WU, Yongdong

Group Art Unit

Examiner Name

Attorney Docket Number

I hereby appoint:

☐ Practitioners at Customer Number

OR

☒ Practitioner(s) named below:

Place Customer  
Number Bar Code  
Label here

Name	Registration Number
JOSEPH H. HANDLEMAN	26179
JOHN RICHARDS	31053
RICHARD J. STREIT	25765
JULIAN H. COHEN	20302

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

<input checked="" type="checkbox"/> Firm or Individual Name	LADAS & PARRY				
Address	26 WEST 61ST STREET				
Address					
City	NEW YORK	State	NY	ZIP	10023
Country	UNITED STATES OF AMERICA				
Telephone	(212) 708-1800	Fax	(212) 246-8959		

I am the:

☒ Applicant.

☐ Assignee of record of the entire interest  
*Certificate under 37 CFR 3.73(b) is enclosed*

**SIGNATURE of Applicant or Assignee of Record**

Name **DENG, Huijie, Robert**

Signature *R. Deng*

Date *24/2/00*

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

EXPRESS MAIL LABEL  
NO.: EL386267783US

Please type a plus sign (+) inside this box ➡ ☐

U 012638-5

Approved for use through 6/30/99. OMB 0651-0035

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**POWER OF ATTORNEY OR  
AUTHORIZATION OF AGENT,  
NOT ACCOMPANYING  
APPLICATION**

Application Number

Filing Date

First Named Inventor

WU, Yongdong

Group Art Unit

Examiner Name

Attorney Docket Number

I hereby appoint:

☐ Practitioners at Customer Number

OR

☒ Practitioner(s) named below:

Place Customer  
Number Bar Code  
Label here

Name	Registration Number
JOSEPH H. HANDLEMAN	26179
JOHN RICHARDS	31053
RICHARD J. STREIT	25765
JULIAN H. COHEN	20302

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

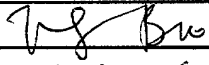
<input checked="" type="checkbox"/> Firm or Individual Name	LADAS & PARRY				
Address	26 WEST 61ST STREET				
Address					
City	NEW YORK	State	NY	ZIP	10023
Country	UNITED STATES OF AMERICA				
Telephone	(212) 708-1800	Fax	(212) 246-8959		

I am the:

☒ Applicant.

☐ Assignee of record of the entire interest  
*Certificate under 37 CFR 3.73(b) is enclosed*

**SIGNATURE of Applicant or Assignee of Record**

Name	BAO, Feng
Signature	
Date	24/02/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

EXPRESS MAIL LABEL  
NO.: EL386267783US